

**3G+ Modem/Router with
Wireless-N and Phone Port
USER MANUAL**



NOTICE

This document contains proprietary information protected by copyright, and this Manual and all the accompanying hardware, software, and documentation are copyrighted. No part of this document may be photocopied or reproduced by mechanical, electronic, or other means in any form.

The manufacturer does not warrant that the hardware will work properly in all environments and applications, and makes no warranty or representation, either expressed or implied, with respect to the quality, performance, merchantability, or fitness for a particular purpose of the software or documentation. The manufacturer reserves the right to make changes to the hardware, software, and documentation without obligation to notify any person or organization of the revision or change.

All brand and product names are the trademarks of their respective owners.

© Copyright 2012

All rights reserved.

Contents

Contents	4
Getting Started	7
Where to Go Next	7
Installing the Hardware	8
Resetting the Modem/Router to the Factory Configuration	9
Using the Modem/Router's Configuration Manager.....	10
Launching the Modem/Router's Configuration Manager	10
Launching the Configuration Manager's Setup Wizard.....	12
Step 1. Setup Login.....	12
Step 2. Setup Time Zone	13
Step 3. WAN Type Setup	14
Selecting the WAN Type.....	14
Step 4. Wireless Settings.....	21
Step 5. Summary	25
Step 6. Finish	26
Connecting Devices Wirelessly to the Modem/Router.....	28
Establishing your Wireless Network.....	28
Connecting a Windows 7 Computer with Built-in Wireless Capabilities...	29
Connecting a Windows Vista Computer with Built-in Wireless Capabilities	30
Connecting a Windows XP Computer with Built-in Wireless Capabilities	31
Connecting a Macintosh OS X Computer with Built-in Wireless Capabilities	32
Connecting a Wireless-enabled Computer or Device (including the iPhone or other cellular phones, the iPod Touch, etc.) to the Modem/Router	33
Connecting a Computer with a Wireless adapter to the Modem/Router	34
Setting up your Network using WPS	35
Configuration Methods	35
Method One	35
Method Two	35
Method Three.....	36
Understanding your Modem/Router's Voice Features	37
Missed Calls.....	38
Received Calls	39
Outgoing Calls	40
Telephone Settings	41
Call Forwarding	42
Call Waiting	43
Speed Dial.....	44
Working with Text Messages.....	45
Using your Modem/Router to Send Text Messages.....	45
Working with your Inbox	47

The Management Settings Page.....	48
Using the Configuration Manager's Advanced Program.....	53
Changing Default Settings	53
Online Help	54
Launching the Configuration Manager's Advanced Program.....	54
Configuring Basic Settings	55
The Basic Setup Page.....	55
Using your 3G+ modem as a Backup	57
The DHCP Server Page.....	58
The Wireless Setting Page	59
WPA2/WPA Configuration	61
WEP Configuration.....	63
The Change Password Page	64
Configuring Forwarding Rules	64
The Virtual Server Page	65
The Port Triggering Page	67
The Miscellaneous Page	68
Configuring Security Settings	69
Status Page	70
Packet Filtering Page	70
The Domain Filters Page	71
The URL Blocking Page	72
The MAC Control Page	73
The VPN-L2TP Client Page.....	74
You can use the VPN-L2TP Client page to set up a L2TP client to securely access your corporate network.....	74
The VPN-PPTP Client Page.....	74
The Miscellaneous Page	75
Configuring Advanced Settings	76
The System Log Page	76
The Dynamic DNS Page	77
The QoS Page	78
The SNMP Page.....	79
The Routing Table Page.....	80
The System Time Page.....	81
The Schedule Rule and Schedule Rule Setting Pages	82
Configuring Toolbox Settings.....	84
The System Information Page.....	84
The Pin Control Page	85
The USSD Page	86
The Firmware Upgrade Page	86
The Backup Setting Dialog	87
The Reset to Default Dialog	87
The Reboot Dialog.....	87
The Miscellaneous Page	88
Appendix A: Mobile Broadband Settings	89

Appendix B: Troubleshooting Tips.....	92
Appendix C: Front Panel Lights	96
Appendix D: Registering Your Product and Getting Help.....	98
Limited Warranty	98
CE Declaration of Conformity.....	100

1

Getting Started

The Modem/Router package contains the 3G+ Modem/Router, a 12V 1.0A Power Cube, an Ethernet cable, a Quick Start flyer, and a CD that contains additional documentation and warranty information. If anything is missing or damaged, please contact Zoom Customer Support or whoever provided the Modem/Router.

Before installing the 3G+ Modem/Router you will need a SIM card for the built-in 3G+ modem. This SIM card may have been provided to you by your service provider or you may need to purchase one. To use the Modem/Router for both data and voice, you will need a SIM that supports both data and voice. If you just want to use the Modem/Router for Internet access, a SIM that only supports data will work.

Where to Go Next

If you have already followed the steps in the Quick Start to install your Modem/Router 3G+ Modem/Router with Phone Port and want to learn how to:

- Add additional wireless devices to your network, go to [Chapter 4: Connecting Devices Wirelessly to the Modem/Router](#).
- Learn about the Modem/Router's voice features including viewing a list of incoming, outgoing or missed calls, or setting up advanced voice features like call forwarding, call waiting, or speed dialing, go to [Chapter 5: Understanding your Modem/Router's Voice Features](#).
- Use the Modem/Router for text messaging, go to [Chapter 6: Working with Text Messages](#).
- Use the Modem/Router's advanced routing features, go to [Chapter 7: Using the Modem/Router's Advanced Features](#). Here you can learn about features such as setting the Modem/Router up for online gaming, changing the default wireless settings including security, backing up your Modem/Router's configuration and setting up scheduling rules to limit when the Modem/Router may be used.

If you have not done the initial setup of your 3G+ Modem/Router with Phone Port, continue on to [Chapter 2: Installing the Hardware](#).

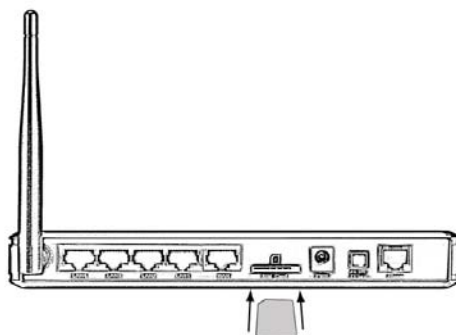
2


Installing the Hardware

This chapter explains installing the Modem/Router hardware. Before installing the hardware you will need a SIM card to use the Modem/Router's cellular modem. If you want to use the Modem/Router for both voice and data you will need a SIM card that supports voice and data. If you just want to use the Modem/Router for data, then you will need a SIM card that at least supports data.


To Install the Modem/Router, follow these steps:

- 1 Place the Modem/Router near a computer to be used for setup. This computer needs an Ethernet (LAN) port.
- 2 Turn off the computer.
- 3 Attach the antenna to the Modem/Router if the antenna isn't already attached. (Remove the antenna from the package. Place the end of the detachable antenna on the open antenna connection port and rotate the antenna clockwise by hand until it no longer turns easily. It may take many turns before the antenna is completely connected). Move the antenna into an upright orientation. The antenna should snap into place.
- 4 Insert the SIM card into the slot on the back of the Modem/Router as shown below. You should hear the SIM card click into place.



- 5 Connect one end of the supplied Ethernet cable to any of the computer's Ethernet ports and the other end to any of the Modem/Router's **LAN** ports.
- 6 Plug the supplied power cube into the Modem/Router, and then into a power outlet. The Modem/Router has completed powering up when the Status light  starts blinking.

Important: Use only the power cube shipped with the Modem/Router. Other power cubes may damage the device.

- 7 Check that the Signal Strength light  has changed from red to green or amber. If the light remains red, please go to [Troubleshooting your Internet Connection](#). A red light means that the Modem/Router can not talk to the mobile broadband network. A green light means you have strong signal, and an amber light means you have a weak signal. If your light is amber, you may try changing the antenna orientation or moving the unit to another location. Normally best cellular performance occurs when the antenna is vertical and when the Modem/Router is not too deep inside a building. For best performance, the Modem/Router should not be on top of a metal surface.
- 8 Turn on the computer. An Ethernet (LAN) LED on your Modem/Router's front panel should light up sometimes, corresponding to the Ethernet (LAN) port you used. If it doesn't light up, please see [Appendix B: Troubleshooting Tips](#).

Resetting the Modem/Router to the Factory Configuration

In the unlikely event that you need to reset the Modem/Router to the factory default configuration, insert the blunt end of a paper clip into the RESET hole on the front panel of the Modem/Router. Hold the clip in place for ten (10) seconds. The Status light will begin blinking rapidly. Once it does release the reset button.

Now continue on to [Chapter 3: Using the Modem/Router's Configuration Manager](#) to configure the Modem/Router.

3

Using the Modem/Router's Configuration Manager

*The Modem/Router includes a built-in Install Wizard that walks you through configuring the Modem/Router's software. For most users running the Install Wizard is all that is needed to configure the Modem/Router. If you are experienced with networking devices and their configuration, you may prefer to use the **Advanced Configuration** program to tailor the Modem/Router's configuration to your needs. In that case go to [Using the Configuration Manager's Advanced Program](#) on page 53.*

Launching the Modem/Router's Configuration Manager

To launch the Configuration Manager, please follow these steps:

- 1 If you haven't already done so, plug the supplied Ethernet cable into the Ethernet port on the Modem/Router's back panel and into your computer's Ethernet port.
- 2 Turn on your Modem/Router first, then your computer. Once the computer is on, launch the computer's Web browser.
- 3 In the computer's Web browser address bar, type the Modem/Router's default IP address, **http://192.168.2.1** and then press **Enter**.

When the **USER'S MAIN MENU** opens for the first time, it displays a **System Status** page that summarizes the current settings and values for your system. If the Status page doesn't appear, please see [Appendix B: Troubleshooting Tips](#).

System Status [HELP]		
Item	WAN Status	Sidenote
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0 , 0.0.0.0	
Connection Time	-	Connecting...
Firmware Version	V1.0.0.1-V-4.	

Wireless Modem Information		
Item	Status	Sidenote
Card Info	HSPA USB MODEM	
Link Status	Connecting...	
Signal Strength	N/A	
Bytes Transmitted	0	
Bytes Received	0	
Network Name		

Wireless Status		
Item	WLAN Status	Sidenote
Wireless mode	Enable	(B/G/N Mixed)
SSID	Zoom_2848DD	
Channel	10	
Security	WPA-PSK / WPA2-PSK	(TKIP/AES)
MAC Address	00:50:18:64:EA:52	

Statistics Information		
Statistics of WAN	Inbound	Outbound
Octets	0	0
Unicast packets	0	0
Multicast packets	0	0
WAN MAC Address	00:50:18:64:EA:51	
LAN MAC Address	00:50:18:64:EA:52	

- 4 On the Toolbar, type **admin** (the default password) in the **System Password** field, then click **Login**.



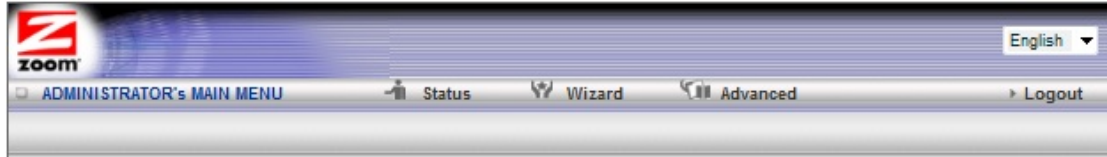
Note: Later, if you change the System Password, you will use the new password to log in.

- 5 By default the configuration manager is set to English. If you wish to change it to Spanish select **Español** from the drop down box on the Toolbar

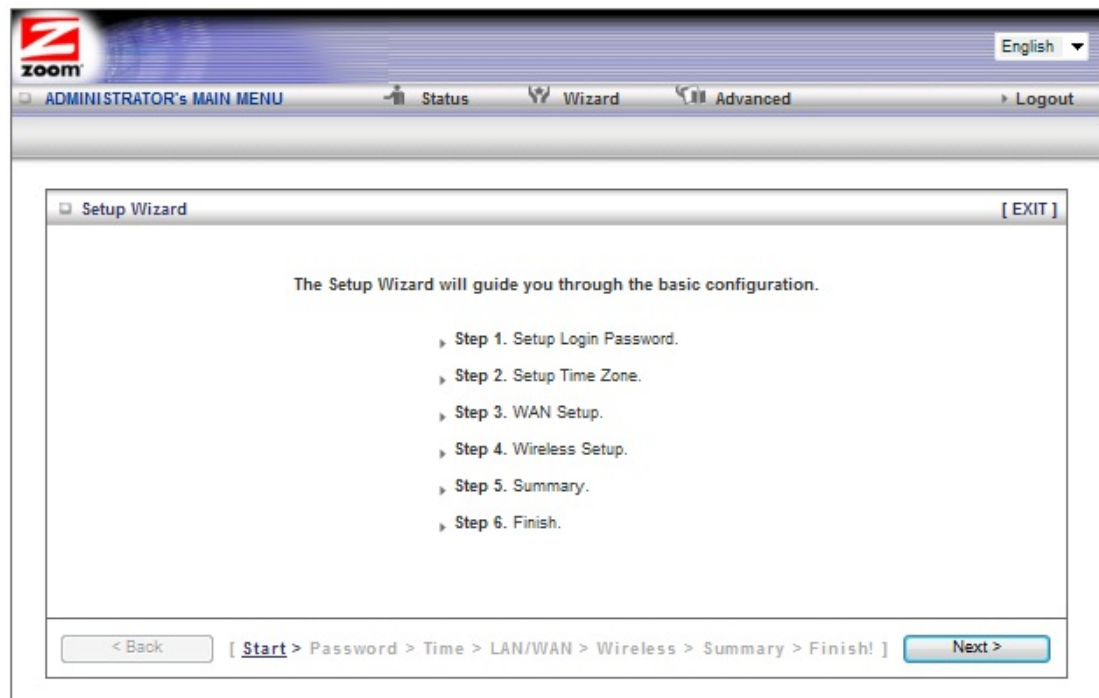
Launching the Configuration Manager's Setup Wizard

When you start the Configuration Manager (<http://192.168.2.1> on your Web browser) and log in, the **ADMINISTRATOR'S MAIN MENU** opens.

Click **Wizard** on the Toolbar to launch the **Setup Wizard**, which will guide you through the configuration process.



The **Setup Wizard** page opens.



Each of the six **Steps** guides you in configuring a specific setting or group of settings. When you click **Next** or **Back**, you move from one step to another. If there is a setting that you don't want to change, simply click **Next** to go to the next setting.

Step 1. Setup Login

To view or change configuration settings, you must enter a password. Your Modem/Router has a default password (**admin**) that was set by the factory and that you used to access the **Configuration Manager** initially. If you want to keep the default password, click **Next** to skip this step. Otherwise, to safeguard your configuration, we **strongly** recommend that you change the login password.

- 1 On the **Setup Login Password** page, type the old password in the **Old Password** field.

- 2 Type the new password in the **New Password** field.
- 3 Type the new password in the **Retype Password** field, then click **Next**.

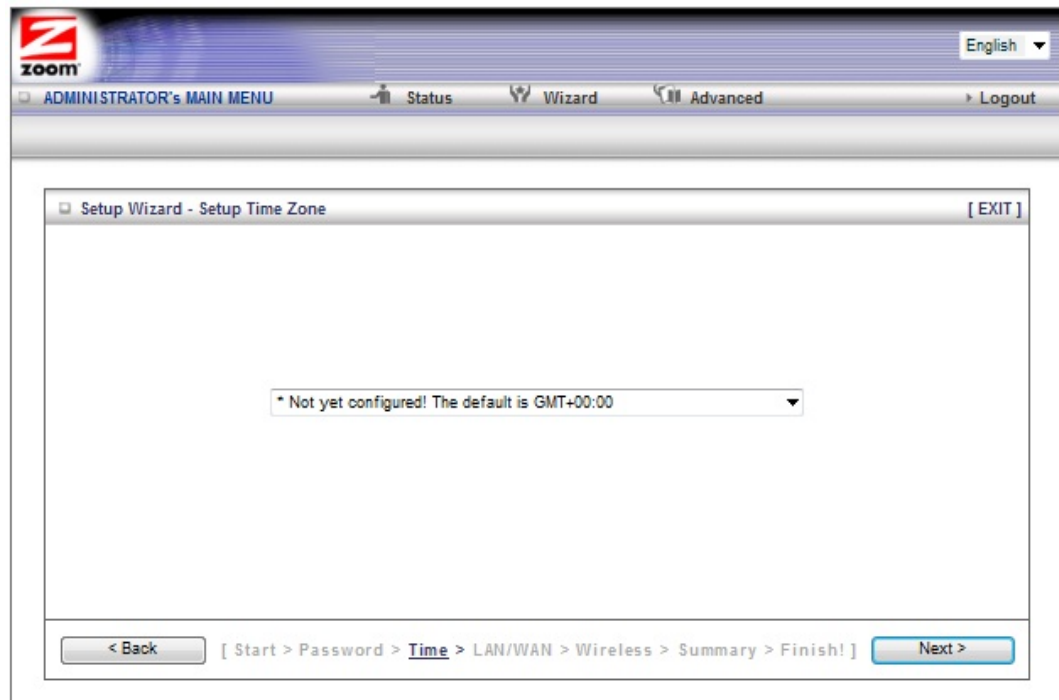
Note: If you forget the new password, you won't have access to the Configuration Manager and will need to restore the device to its factory settings, thus losing any changes you made to your Modem/Router's configuration. To avoid this problem, we recommend that you write the new password here and on the bottom of your Modem/Router, and also save it elsewhere such as a settings document.

PASSWORD: _____

Please refer to [Resetting the Modem/Router to the Default Configuration](#) on page 9 or [The Reset to Default Dialog](#) on page 87 for more information in the unlikely event that you need to restore the Modem/Router's default settings.

Step 2. Setup Time Zone

The **Time Zone** setting is used to track your incoming, outgoing, and missed calls, and for fairly sophisticated functions, such as changing Modem/Router access rules depending on the time of day. We recommend that you set your time zone now.

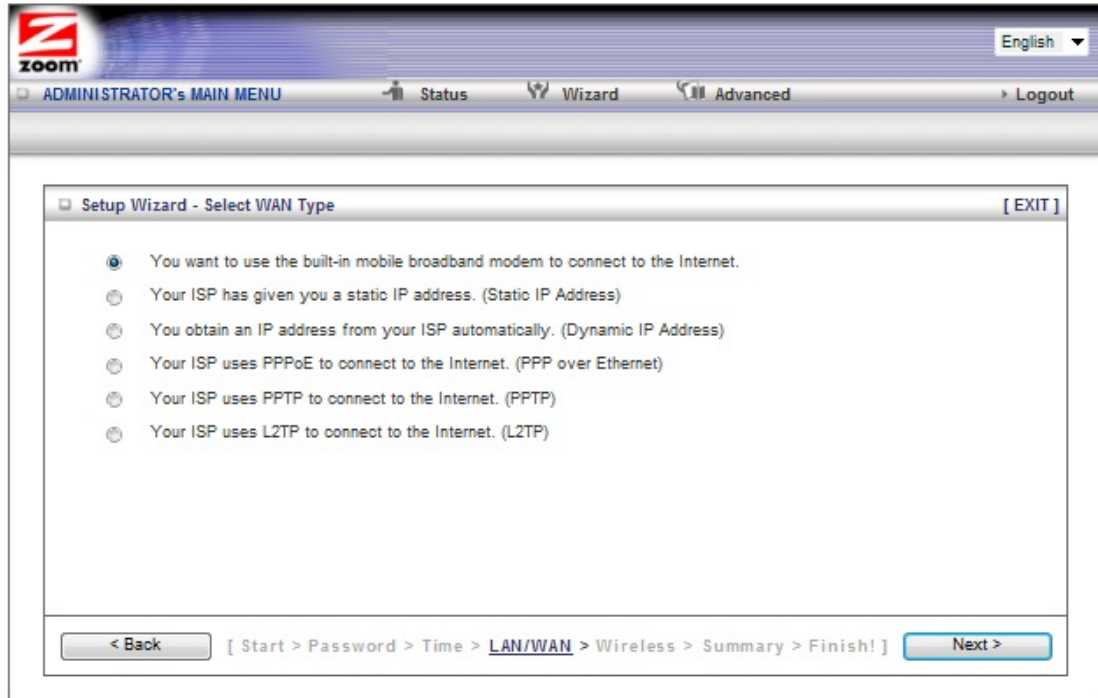


The screenshot shows the Zoom Configuration Manager interface. At the top is the Zoom logo and a language dropdown set to 'English'. Below this is a navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area is titled 'Setup Wizard - Setup Time Zone' with an '[EXIT]' button. In the center is a dropdown menu with the text '* Not yet configured! The default is GMT+00:00'. At the bottom, there is a '< Back' button, a breadcrumb trail '[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]', and a 'Next >' button.

To set the time zone, select the time zone that applies to your location from the dropdown menu, and then click **Next**.

Step 3. WAN Type Setup

The **WAN Type** refers to the protocol used by your Internet Service Provider in establishing your Internet connection. By default, **WAN Type** is set to use the built-in mobile broadband modem. If that is what you want, you can select **Next** to skip this section.



Selecting the WAN Type

Please check with your service provider if you read the discussion below and are still unsure which **WAN Type** to choose.

- [Mobile Broadband Modem](#) - Select this if you want to use the Modem/Router's built-in 3G+ modem for voice and data. (If you want to use the 3G+ modem as the backup to an ADSL or Cable modem, you'll need to use the Configuration Manager's **Advanced** program to configure this setup. Please refer to **3G Failover** on [The Basic Setup Page](#) on page 55.) You should select your primary connection type using the Setup Wizard. (To access the Setup Wizard, refer to page 12 for instructions.)
- [Configuring the Dynamic IP Address](#) – This is only used by Cable modem users and by DSL modem users who are not using PPPoE. (ADSL service providers will typically tell you whether you are using PPPoE, which requires you to enter an PPPoE-related password into the Modem/Router. If you are using ADSL with 1483 routed, bridged, or PPPoA modes, you are not using PPPoE.)
- [Static IP Address](#) - Typically you have to request and pay extra for a static IP address, so this is not typically used.
- [PPPoE](#) – Only use this if you are plugging an ADSL modem into the

Modem/Router, and if your ADSL service provider uses PPPoE.

- [PPTP](#) - The Point to Point Tunneling Protocol is more common in corporate environments and most users will not use this setting.
- [L2TP](#) - The Layer 2 Tunneling Protocol is more common in corporate environments and most users will not use this setting.

The relevant section immediately below depends on the WAN Type you selected.

Configuring the Built-in 3G+ Modem

The page shown below only appears if you select the **Built-in Mobile Broadband modem** button on the **Select WAN Type** menu. Otherwise skip this section.

The screenshot shows the 'Setup Wizard - 3G+' window. At the top, there's a navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The 'Wizard' tab is active. Below the navigation bar, the 'Setup Wizard - 3G+' window has a title bar with a close button and '[EXIT]'. Inside the window, there are two sections: 'Profile' and 'PIN Code'. Under 'Profile', there are two radio buttons: 'Auto-Detection' (which is selected) and 'Manual'. Under 'PIN Code', there is a text input field followed by '(optional)'. At the bottom of the window, there is a progress bar with the following steps: '< Back', '[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]', and 'Next >'. The 'LAN/WAN' step is currently highlighted.

On the **Setup 3G+** page, **Auto-Detection** is enabled by default to automatically detect your SIM card provider. A message will show whether auto-detection was successful or not. If auto-detection was successful, click **Next**. If auto-detection failed to detect your SIM card provider, click **OK** to close the message box and then select **Manual Setup**. On the **Manual Setup** page select your **Country**, and then select the name of your **Service Provider** from the drop down list. The rest of the fields on the page are automatically filled in. If a field is left empty, don't worry since that field is not used for your provider. Click **Next**.

Note: If your country or service provider does not appear in the dropdown list you must manually enter your service providers settings. This can be done by selecting **Manual Setup** and entering your settings manually or by using the **Basic Setup** page. Please see [Chapter 7. Using the Configuration Manager's Advanced Program](#) for how to configure the **Basic Setup** page.

Go to [Step 4. Wireless Settings](#).

Configuring the Static IP Address

The page shown below will only appear in the unlikely event that you select the **Static IP Address** button on the **Select WAN Type** menu. Otherwise skip this section.

The screenshot shows the Zoom! web interface. At the top is the Zoom! logo and a language dropdown set to 'English'. Below this is a navigation bar with 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area is titled 'Setup Wizard - Static IP Address' with an '[EXIT]' button. It contains five fields for configuration: 'Static IP Address', 'Static Subnet Mask', 'Static Gateway', 'Static Primary DNS', and 'Static Secondary DNS'. At the bottom, there is a '< Back' button, a progress bar showing the sequence '[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]', and a 'Next >' button.

- **Static IP Address**

This is the IP address that is given to you by your service provider when you sign up for a Static IP address. This address identifies your Modem/Router when seen from the Internet.

- **Static Subnet Mask**

This is the Modem/Router's **subnet mask**. Your service provider supplies this address.

- **Static Gateway**

This is the **IP address of the ISP Gateway**. Your service provider supplies this address.

- **Static Primary DNS**

This is the Domain Name System (**DNS**) server's IP address. Your service provider supplies this address.

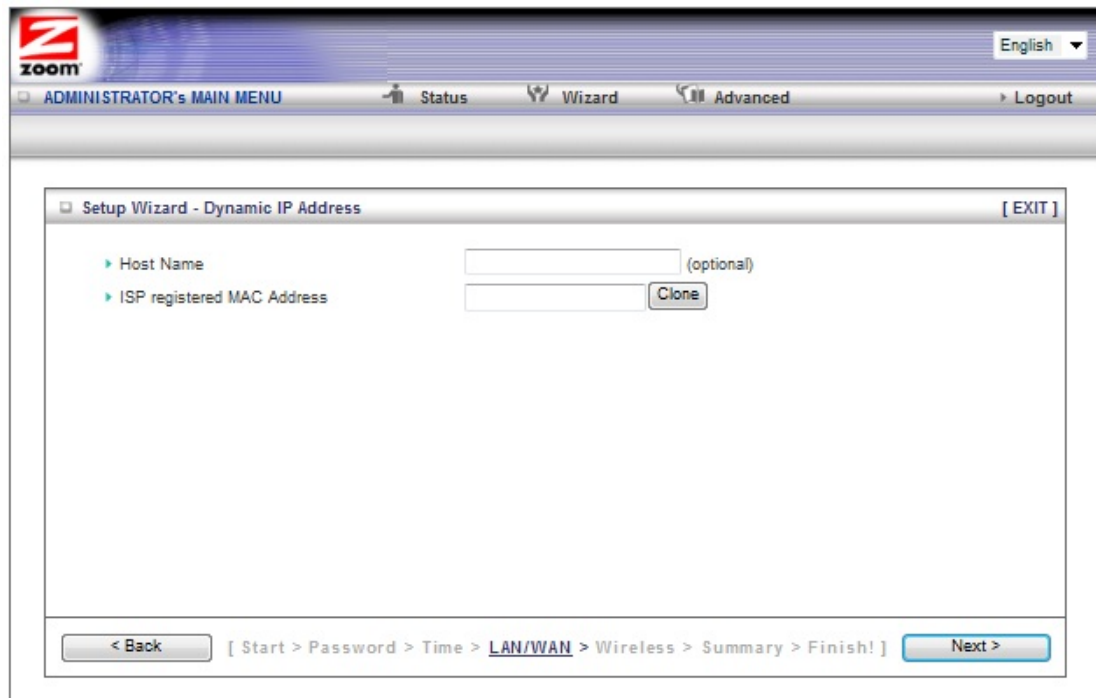
- **Static Secondary DNS**

This is the IP address of an alternate Domain Name System (**DNS**) server. Your service provider supplies this address.

Go to [Step 4. Wireless Settings](#) on page 21.

Configuring the Dynamic IP Address

The page shown below only appears if you select the **Dynamic IP Address** button on the **Select WAN Type** menu. Otherwise skip this section.



The screenshot shows the Zoom! Setup Wizard interface. At the top, there is a navigation bar with the Zoom! logo, a language dropdown set to 'English', and links for 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area is titled 'Setup Wizard - Dynamic IP Address' and includes an '[EXIT]' link. It contains two configuration options: 'Host Name' with a text input field and '(optional)' label, and 'ISP registered MAC Address' with a text input field and a 'Clone' button. At the bottom, there is a progress bar with buttons for '< Back' and 'Next >', and a breadcrumb trail: '[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]'.

- **Host Name**

This is the name that identifies your Modem/Router. Some service providers require a host name. Your service provider supplies this name, if needed.

- **ISP registered MAC Address**

This is the 12-digit **Media Access Control (MAC)** address of your Modem/Router. Cable modem users should click the **Clone** button to get the MAC address that was registered with your service provider for your device.

Go to [Step 4. Wireless Settings](#) on page 21.

Configuring PPPoE

The page shown below only appears if you select the **PPPoE** button on the **Select WAN Type** menu. Otherwise skip this section.

The screenshot shows the 'Setup Wizard - PPP over Ethernet' window. At the top, there is a 'zoom!' logo and a language dropdown set to 'English'. Below this is a navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area lists six configuration items, each with a corresponding input field: 'PPPoE Account', 'PPPoE Password', 'Primary DNS', 'Secondary DNS', 'Service Name (optional)', and 'Assigned IP Address (optional)'. At the bottom, there is a progress bar showing the sequence: '[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]'. Navigation buttons include '< Back' and 'Next >'.

- **PPPoE Account**

This is the PPPoE username supplied by your service provider.

- **PPPoE Password**

This is PPPoE password supplied by your service provider.

- **Primary DNS**

This is the Domain Name System (DNS) server's IP address. Your service provider supplies this address, if needed. Most users should not need to enter a DNS value.

- **Secondary DNS**

This is the IP address of an alternate Domain Name System (DNS) server. Your service provider supplies this address, if needed.

- **Service Name**

This is the name assigned by your service provider to identify your service. The **Service Name** is optional.

- **Assigned IP Address**

This is the optional IP address assigned by your service provider. The **Assigned IP Address** is optional.

Go to [Step 4. Wireless Settings](#) on page 21.

Configuring PPTP

The page shown below only appears if you select the **PPTP** button on the **Select WAN Type** menu. Otherwise skip this section.

The screenshot shows the Zoom Administrator's Main Menu. At the top, there is a navigation bar with the Zoom logo, a language dropdown set to 'English', and links for 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area displays the 'Setup Wizard - PPTP' window. This window has a list of configuration steps on the left: 'IP Mode', 'My IP Address', 'My Subnet Mask', 'Gateway IP', 'Server IP Address/Name', 'PPTP Account', and 'PPTP Password'. The 'IP Mode' dropdown menu is currently set to 'Dynamic IP Address'. Below the list, there are input fields for each step. At the bottom of the wizard, there is a '< Back' button, a progress indicator '[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]', and a 'Next >' button.

- **IP Mode**

This is the mode used to generate the IP address. Select an option from the dropdown menu, based on your service provider's requirements.

- **My IP Address**

This is the private IP address that your service provider assigned to your Modem/Router. Only used if **Static IP Address** is selected as the **IP Mode**.

- **My Subnet Mask**

This is the private subnet mask that your service provider assigned to your Modem/Router. Only used if **Static IP Address** is selected as the **IP Mode**.

- **Gateway IP**

This is the IP address of the service provider's server. Your service provider supplies this address. Only used if **Static IP Address** is selected as the **IP Mode**.

- **Server IP Address/Name**

This is the name and IP address of the PPTP server. Your service provider supplies this information, if needed.

- **PPTP Account**

This is the PPTP account name that your service provider assigned to you.

- **PPTP Password**

This is PPTP password that your service provider assigned to you.

Go to Go to [Step 4. Wireless Settings](#) on page 21.

Configuring L2TP

The page shown below only appears if you select the **L2TP** button on the **Select WAN Type** menu. Otherwise skip this section.

The screenshot shows the 'Setup Wizard - L2TP' window within the Zoom Administrator's Main Menu. The window has a title bar with the Zoom logo and a language dropdown set to 'English'. Below the title bar is a navigation bar with links: 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area is titled 'Setup Wizard - L2TP' and contains a list of configuration options on the left and input fields on the right. The options are: 'IP Mode' (with a dropdown menu currently showing 'Dynamic IP Address'), 'IP Address', 'Subnet Mask', 'WAN Gateway IP', 'Server IP Address/Name', 'L2TP Account', and 'L2TP Password'. At the bottom of the window is a progress bar with buttons for '< Back' and 'Next >', and a breadcrumb trail: '[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]'.

- **IP Mode**

This is the mode used to generate the IP address. Select an option from the dropdown menu, based on your service provider's requirements.

- **IP Address**

This is the IP address that identifies the L2TP server. Your service provider supplies this address. Only used if **Static IP Address** is selected as the **IP Mode**.

- **Subnet Mask**

This is the Modem/Router's subnet mask. Your service provider supplies this address. Only used if **Static IP Address** is selected as the **IP Mode**.

- **WAN Gateway IP**

This is the WAN Gateway IP address of the L2TP server. Your service provider supplies this address. Only used if **Static IP Address** is selected as the **IP Mode**.

- **Server IP Address/Name**

This is the name and IP address of the L2TP server. Your service provider supplies this information, if needed.

- **L2TP Account**

This is the L2TP account name or user name supplied by your service provider.

- **L2TP Password**

This is L2TP password supplied by your service provider.

Go to [Step 4. Wireless Settings](#) on page 21.

Step 4. Wireless Settings

The **Wireless Settings** page lets you change the wireless settings for your Modem/Router. If you are happy with your wireless settings (set at the factory to wireless with WPA2/WPA security), click **Next** to go to Step 5. Otherwise, continue below. EITHER WAY, after running the Setup Wizard you will need to make sure that wireless devices connecting to the Modem/Router (computers, phones, tablets, game stations, etc.) are set up properly as discussed in [Chapter 3](#).

The screenshot shows the 'Setup Wizard - Wireless settings' window. At the top, there is a 'zoom' logo and a language dropdown set to 'English'. Below the logo is a navigation bar with links: 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area has a title bar 'Setup Wizard - Wireless settings' and an '[EXIT]' button. Inside, there are three settings: 'Wireless Function' with 'Enable' selected, 'Wireless Network Name (SSID)' with the value 'Zoom_2848DD', and 'Channel' with a dropdown menu showing '10'. At the bottom, there is a progress bar with buttons '< Back' and 'Next >', and a text string '[Start > Password > Time > LAN/WAN > **Wireless** > Summary > Finish!]'.

- **Wireless Function** Accept the default, **Enable**. Click the **Disable** checkbox only if you do not want wireless clients to access your network.
- **Wireless Network Name (SSID)** is the name of your wireless network. By default, the SSID for the Modem/Router is **Zoom-xxxxxx**, where xxxxxx is 6 random alphanumeric digits. Your default SSID is printed on the label on the bottom of your unit. You can change the SSID to a name of your choice. The **SSID** can be up to 32 alphanumeric characters. If you change the name, make sure that all devices on your Modem/Router's wireless network use the new SSID as the access point.
- **Channel** refers to the wireless network channel assigned to your LAN. By

default, the Modem/Router uses channel **10**. You would only change this setting if you were concerned about possible interference from another wireless access point using the same channel.

TIP: Other wireless networks might be within range of your network. Your neighbors, for instance, may be within range. If you are having trouble connecting, try setting a different channel to see if that improves performance. You should try setting a channel that is 5 or more channels away from what you are using. By default, the Modem/Router is set to 10. You may want to try channel 1 or 6, for instance, if you have trouble connecting with the default channel (10).

Wireless Security Settings

If you accepted the default to **Enable** the **Wireless Function** (on the **Wireless Settings** page at Step 4), the following page opens when you click **Next**.

Configuring Authentication and Encryption

By default, **Authentication** and **Encryption** security services are set to **WPA2/WPA** and a random **Security Key** is programmed in at the factory. This key is printed on the label on the bottom of your unit. Most users should accept the default settings.

If you have devices on your network that only support WEP (for example, some gaming consoles) than you will need to setup WEP. Please see [WEP Authentication and Encryption](#).

If you want to change the **Security Key** used by the Modem/Router. For example, you are replacing an existing wireless Modem/Router and want to use the same key. Enter the key you want to use in the **Security Key** field. This key should be from 8 to 64 characters long.

Important: If you are attaching other wireless devices to your Modem/Router you will need to enter the **Security Key** that is printed on the bottom label on your Modem/Router. If you have changed this key, you will need to enter the new key. See [Chapter 4: Connecting Devices Wirelessly to the Modem/Router](#) for more information.

WEP Authentication and Encryption

If you have devices on your wireless network that support only **WEP**, (for example, some gaming consoles), you will need to select **WEP** as your **Authentication** method.

When you select **WEP** from the **Authentication** dropdown menu, the **Encryption** field expands, as shown in the following figure.

Field	Entry
Authentication	Select WEP
Encryption	Select WEP
Encryption WEP Key 1, 2, 3, 4	We recommend selecting HEX as the key format as Ascii keys can have compatibility issues between different devices..

Encryption WEP Key 1, 2, 3, 4	<p>You can choose to either use WEP 128 bit encryption or WEP 64 bit encryption. The difference is 128 bit is more secure and 64 bit is faster. We recommend selecting 64 bit.</p> <p><i>If you selected Hex format and you chose a 64-bit key length, 10 hexadecimal values are required. (Hexadecimal values include the numbers 0-9 and the letters A-F) Write the 10-hexadecimal key in the space below for future reference, and then enter it in the Key 1 box.</i></p> <p>_____</p> <p><i>If you selected Hex format and you chose a 128-bit key length, 26 hexadecimal values are required. (Hexadecimal values include the numbers 0-9 and the letters A-F) Write the 26-hexadecimal key in the space below for future reference, and then enter it in the Key 1 box.</i></p> <p>_____</p> <p>_____</p> <p><i>If you selected ASCII format, and you chose a 64-bit key length, 5 ASCII characters are required. Write the 5-ASCII-character key in the space below for future reference, and then enter it in the Key 1 box.</i></p> <p>_____</p> <p><i>If you selected ASCII format, and you chose a 128-bit key length, 13 ASCII characters are required. Write the 13-ASCII-character key in the space below for future reference, and then enter it in the Key 1 box.</i></p> <p>_____</p>
--	---

Step 5. Summary

The **Summary** page displays the updated configuration settings for your Modem/Router and lets you accept, change, and test the configured values.

The screenshot shows the 'Setup Wizard - Summary' page of a Zoom Modem/Router. The page has a header with the Zoom logo, a language dropdown set to 'English', and navigation links: 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area is titled 'Please confirm the information below' and contains two sections: '[WAN Setting]' and '[Wireless Setting]'. The WAN settings include WAN Type (3G+), APN (ISP.CINGULAR), PIN Code, Dialed Number (*99#), Username, and Password (masked with asterisks). The Wireless settings include Wireless (Enable), SSID (Zoom_2848DD), Channel (10), Authentication (WPA-PSK / WPA2-PSK), and Encryption (TKIP/AES). Below these settings is a checkbox labeled 'Do you want to proceed with the network testing?' which is checked. At the bottom, there is a '< Back' button, a breadcrumb trail '[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]', and an 'Apply Settings' button.

[WAN Setting]	
WAN Type	3G+
APN	ISP.CINGULAR
PIN Code	
Dialed Number	*99#
Username	
Password	*****

[Wireless Setting]	
Wireless	Enable
SSID	Zoom_2848DD
Channel	10
Authentication	WPA-PSK / WPA2-PSK
Encryption	TKIP/AES

☒ Do you want to proceed with the network testing?

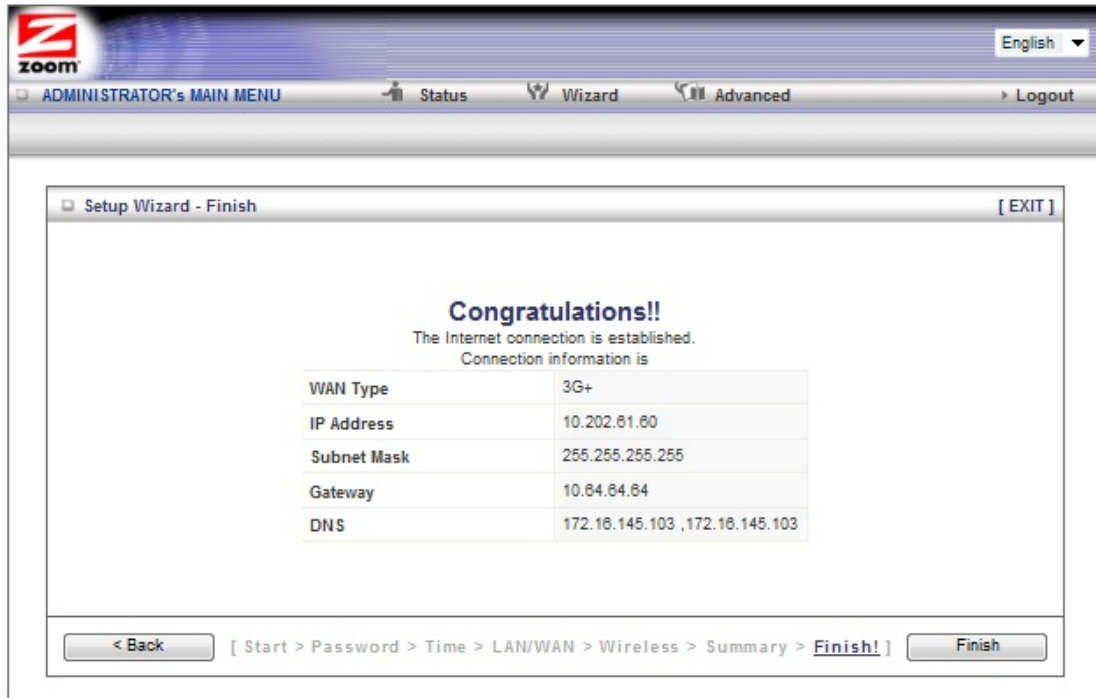
< Back [Start > Password > Time > LAN/WAN > Wireless > **Summary** > Finish!] Apply Settings

- 1 To edit your entries, click **Back** as many times as needed to access the page for the field(s) to be edited, then click **Next** to continue with your edits or to return to the updated **Summary** page.
- 2 **If you are using the built-in 3G+ Modem** the **Do you want to proceed with the network testing?** check box is selected. We recommend that you leave this checked to test your 3G+ connection. If you do not want to test your 3G+ connection at this time uncheck the **Do you want to proceed with the Network testing box**.
Note: If you are not using the built-in 3G+ modem this option does not appear.
- 3 When you're satisfied with the configured settings, click **Apply Settings** to save the new configuration.

Step 6. Finish

If you are not using the built-in 3G+ modem or you decided not to test your mobile broadband connection the **Configuration is Completed** page displays. Click **Finish** to restart the Modem/Router and save the new configuration settings.

If your Internet connection test was successful, the **Congratulations!!** screen will appear. Click **Finish** to restart the Modem/Router and save the new configuration settings.



If your Internet connection test was not successful, try running the test again by clicking **Connect Again**. If the test still fails please see [Troubleshooting your Built-in 3G+ Modem Connection](#).


Congratulations! Your Modem/Router should now be configured.

- If you want to learn how to attach other wireless devices to the Modem/Router go to [Chapter 4: Connecting Devices Wirelessly to the Modem/Router](#).
- If you want to learn about the Modem/Router's voice features including viewing a list of incoming, outgoing or missed calls, or setting up advanced voice features like Call forwarding, call waiting, or speed dialing go to [Chapter 5: Understanding your Modem/Router's Voice Features](#).
- To learn how to use the Modem/Router for text messaging go to [Chapter 6: Working with Text Messages](#).
- In the unlikely event that you want to use the **Advanced** configuration program to tailor the Modem/Router's configuration to your needs, for

example, to set up a Virtual Server or DMZ so that your games or gaming consoles can access the Internet through your Modem/Router's firewall, please continue to [Chapter 7: Using the Configuration Manager's Advanced Program](#). (Most users will not need to do this.)

Your Modem/Router's setup is complete. **Congratulations!**

Troubleshooting your Built-in 3G+ Modem Connection

If you are unable to connect to the Internet through your Modem/Router, please first check Signal Strength light  on the Modem/Router's front panel.

If the light is red that means either your SIM card is not inserted or not working, or your Modem/Router is not receiving a mobile broadband signal. If your Signal Strength light is red please try the following:

- Check that your SIM card is properly inserted into the back of your Modem/Router.
- Verify that you are in a mobile broadband coverage area. You may want to move the antenna to optimize signal strength; putting the antenna in a vertical position normally gives the best performance. You may also want to try changing the location of your Modem/Router, for example, by moving the Modem/Router closer to a window.

If your Signal Strength Light is amber or green that means you are connected to the mobile broadband network but most likely your mobile broadband settings are wrong. If your Signal Strength light is green or amber please try the following:

- If you used auto-configure to detect your service provider, the Modem/Router may have used the wrong settings for your provider. Auto-configure can detect your service provider, but it cannot detect the actual settings. Once it detects your provider it tries the most common setting for that provider. To check if this is the problem, run the setup wizard again. When you get to the **Setup 3G+** page select **Manual**. Select your country and then select your service provider. If you have multiple settings for your service provider you will need to run the wizard again until you have tried each setting. If none of the predefined settings work, contact your service provider and ask if they can provide you with your **APN, Dialed Number, Username, Password, and Pin Code**. Some of these settings are optional and your service provider may not need them.
- If your Signal Strength light is amber, you may want to move the antenna to optimize signal strength; putting the antenna in a vertical position normally gives the best performance. You may also want to try changing the location of your Modem/Router, for example, by moving it closer to a window.

If you are still having problems connecting to the Internet please contact Zoom Technical Support as described in [Appendix E: Registering Your Product and Getting Help](#).

4

Connecting Devices Wirelessly to the Modem/Router

*This chapter provides tips for connecting devices (computers, phones, tablets, game stations, etc.) wirelessly to the Modem/Router. If you are familiar with this already, **or if you prefer to use the instructions associated with each device**, you don't need to read this chapter. You do need to make sure that each device connecting to the Modem/Router is set up for wireless security that is compatible with the Modem/Router's wireless security settings.*

Establishing your Wireless Network

Note that for **each** computer or other device added to your wireless network, you will need to take appropriate steps for setting up that computer or other device. To do that, select one of the possibilities for that computer or other device below:

- Many newer **Windows 7, Vista, and XP computers have built-in wireless networking** capabilities and do not require the installation of a wireless component. If this is the case, you should set up that computer's wireless connection using the Windows 7, Vista, or XP connect utility. See the sections below on connecting **Windows 7** (page 29) , **Vista** (page 30), or **XP** (page 31) computers with built-in wireless capabilities.
- Some **computers** may have **built-in wireless networking** capabilities, but do not use the Windows 7, Vista, or XP utility to configure their device. If this is so, set up your computer's wireless connection using the instructions on page 31 for **Connecting a Wireless-enabled Computer or Device to the Modem/Router**.
- If you are using a Macintosh computer see the instructions on page 32 for **Connecting a Macintosh OS X Computer with Built-in Wireless Capabilities**
- If you have a non-computer **wireless device like an iPhone or other cellular phone, iPod Touch**, etc., see the instructions on page 31 for **Connecting a Wireless-enabled Computer or Device to the Modem/Router**.
- Some **computers** may need a **wireless network adapter installed**. This can be a USB adapter, PC Card adapter, or PCI adapter. When you install the adapter, make sure that it is set to **infrastructure** or **access point** mode (NOT **ad-hoc** or **peer-to-peer** mode). If you need help installing your wireless adapter or setting its mode, refer to the documentation that came with it. After you install the adapter, see the

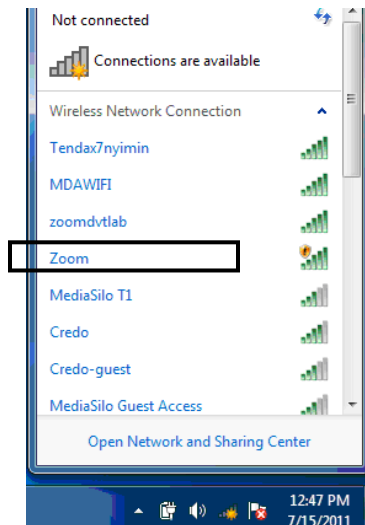
instructions on page 31 for **Connecting a Computer with a wireless adapter to the Modem/Router**.

Connecting a Windows 7 Computer with Built-in Wireless Capabilities

- 1 From the taskbar, click on the wireless symbol.



- 2 In the wireless network options box, highlight the Wireless Network Name (SSID) you gave your wireless network in Step 4 of the Setup Wizard. If you did not change the Wireless Network Name (SSID), select the default name **Zoom_xxxxxx**, where xxxxxx are 6 random alphanumeric characters. The complete Wireless Network Name is printed on the bottom label of your unit. If you want to automatically connect to the Modem/Router, click the **Connect Automatically** box. Then click **Connect**.



- When prompted, enter the **Security Key** found on the bottom label of your unit. If you changed the key in Step 4 of the Setup Wizard, enter the new security key and click **Connect**.
 - If you disabled wireless security in Step 4 of the Setup Wizard select **Connect Anyway** when warned that your network is unsecure.
- When you click on the wireless network option box, Windows will scan for available networks. More than one wireless network may appear in the list. These are other wireless networks that are within range of your network. Your neighbors, for instance, may be within range of your network. Each wireless network has a channel associated with it. We recommend there be at least a five-channel difference between your network and those of your neighbors. Having less than a five-channel difference may result in interference with your connection. By default, the Modem/Router uses channel 10. If you need to change this channel, you must do so using the **Wireless Setup** page of the **Zoom Configuration Manager**. For instructions on how to log in to the **Zoom Configuration Manager**, see page 10. After logging in, select **Wireless** from the left-hand menu. On the **Wireless** page you can select a new channel from the drop-down menu.

To disconnect from the current network:

- 1 Right-click the wireless network icon in the notification area of the Windows taskbar.
- 2 Right-click your Wireless Network Name and select **Disconnect**.

Connecting a Windows Vista Computer with Built-in Wireless

Capabilities

- 1 From the **Start** menu select **Connect to**.
 - 2 In the wireless network options box, highlight the Wireless Network Name (SSID) you gave your wireless network in Step 4 of the Setup Wizard. If you did not change the Wireless Network Name (SSID), select the default name **Zoom_XXXXXX**, where XXXXXX are 6 random alphanumeric characters. The complete Wireless Network Name is printed on the bottom label of your unit. If you want to automatically connect to the Modem/Router, click the **Connect Automatically** box. Then click **Connect**.
 - When prompted, enter the **Security Key** found on the bottom label of your unit. If you changed the key in Step 4 of the Setup Wizard, enter the new security key and click **Connect**.
 - If you disabled wireless security in Step 4 of the Setup Wizard select **Connect Anyway** when warned that your network is unsecure.
- When you click on the wireless network option box, Windows will scan for available networks. More than one wireless network may appear in the list. These are other wireless networks that are within range of your network. Your neighbors, for instance, may be within range of your network. Each wireless network has a channel associated with it. We recommend there be at least a five-channel difference between your network and those of your neighbors. Having less than a five-channel difference may result in interference with your connection. By default, the Modem/Router uses channel 10. If you need to change this channel, you must do so using the **Wireless Setup** page of the **Zoom Configuration Manager**. For instructions on how to log in to the **Zoom Configuration Manager**, see page 10. After logging in, select **Wireless** from the left-hand menu. On the **Wireless** page you can select a new channel from the drop-down menu.
- 3 In the **Successfully connected to [desired network]** dialog box, you have three options. You can:
 - Select **Save the network** and **Start this connection automatically** if you always want to connect to the same network. Then click **Close**. The next time you start your computer you will automatically connect to the selected network.
 - Select **Save the network** and clear the **Start this connection automatically** check box if you don't want to automatically connect to this network every time you start your computer but you will want to connect in the future. Click **Close** to display the **Select a location . . .** dialog box where you choose a location. Windows Vista automatically applies the correct network security settings. If the **User Account Control** dialog box appears, click **Continue**.
 - Click **Close** to complete the connection procedure. Select this option if you are connecting to this network only one time.

To disconnect from the current network:

- 1 From the **Start** menu, select **Connect to**.
- 2 In the **Disconnect or Connect to another network** dialog box, select the current network and click **Disconnect**.
- 3 In the **Are You Sure?** message box, click **Disconnect** again.
- 4 In the next dialog box, you can connect to another network or click **Close** to complete the disconnect procedure.

Connecting a Windows XP Computer with Built-in Wireless Capabilities

- 1 On your Windows desktop, click the **Wireless Network Icon** in the System Tray.
 - 2 In the wireless network options box, highlight the Wireless Network Name (SSID) you gave your wireless network in Step 4 of the Setup Wizard. If you did not change the Wireless Network Name (SSID), select the default name **Zoom_XXXXXX**, where XXXXXX are 6 random alphanumeric characters. The complete Wireless Network Name is printed on the bottom label of your unit. If you want to automatically connect to the Modem/Router, click the **Connect Automatically** box. Then click **Connect**.
 - When prompted, enter the **Security Key** found on the bottom label of your unit. If you changed the key in Step 4 of the Setup Wizard, enter the new security key and click **Connect**.
 - If you disabled wireless security in Step 4 of the Setup Wizard select **Connect Anyway** when warned that your network is unsecure.
- When you click on the wireless network option box, Windows will scan for available networks. More than one wireless network may appear in the list. These are other wireless networks that are within range of your network. Your neighbors, for instance, may be within range of your network. Each wireless network has a channel associated with it. We recommend there be at least a five-channel difference between your network and those of your neighbors. Having less than a five-channel difference may result in interference with your connection. By default, the Modem/Router uses channel 10. If you need to change this channel, you must do so using the **Wireless Setup** page of the **Zoom Configuration Manager**. For instructions on how to log in to the **Zoom Configuration Manager**, see page 10. After logging in, select **Wireless** from the left-hand menu. On the **Wireless** page you can select a new channel from the drop-down menu.

To disconnect from the current network:

- 1 On your Windows desktop, click the **Wireless Network Icon** in the System Tray.
- 2 **Select** your Wireless Network Name. And click on **Disconnect**.

Connecting a Macintosh OS X Computer with Built-in Wireless

Capabilities

- 1 Click the Wi-Fi icon in the menu bar. If the Wi-Fi icon does not appear on your menu bar please refer to your built-in documentation on how to enable wireless.



Note: On versions prior to OS 10.7 the **Wi-Fi** icon is called **AirPort**.

- 2 Select the Wireless Network Name (SSID) you gave your wireless network in Step 4 of the Setup Wizard. If you did not change the Wireless Network Name (SSID), select the default name **Zoom_XXXXXX**, where XXXXXX is 6 random alpha numeric characters.
 - When prompted for the wireless password, enter the **Security Key** found on the bottom label of your unit. If you changed the key in Step 4 of the Setup Wizard, enter the new security key. Click **OK** to connect to the Modem/Router.
- More than one wireless network may appear in the list. These are other wireless networks that are within range of your network. Your neighbors, for instance, may be within range of your network. Each wireless network has a channel associated with it. We recommend there be at least a five-channel difference between your network and those of your neighbors. Having less than a five-channel difference may result in interference with your connection. By default, the Modem/Router uses channel 10. If you need to change this channel, you must do so using the **Wireless Setup** page of the **Zoom Configuration Manager**. For instructions on how to log in to the **Zoom Configuration Manager**, see page 10. After logging in, select **Wireless** from the left-hand menu. On the **Wireless** page you can select a new channel from the drop-down menu.

To disconnect from the current network:

- 1 Click the Wi-Fi icon on the menu bar.
- 2 Select **Turn Wi-Fi Off** (OS 10.7 or later) or **Turn AirPort Off** (OS versions prior to 10.7) to disconnect from the Modem/Router.

Connecting a Wireless-enabled Computer or Device (including the iPhone or other cellular phones, the iPod Touch, etc.) to the Modem/Router

- 1 Go to the wireless-enabled computer or device that you want to add to the network. The device should have software that will let it perform a **site search** to scan for available wireless networks in your area. You may have to click on something like **Settings** and then **Wi-Fi**. When the Wireless Network Name (SSID) (Service Set Identifier) that you gave the Modem/Router Step 4 of the Setup Wizard. If you did not change the Wireless Network Name (SSID), select the default name **Zoom_xxxxxx**, where xxxxxx are 6 random alphanumeric characters. The complete Wireless Network Name is printed on the bottom label of your unit. Select it as the network you want to use to connect to the Internet.

When prompted, enter the **Security Key** found on the bottom label of your unit. If you changed the key in Step 4 of the Setup Wizard, enter the new security key and click **Connect**.

Tip!

If you need help, refer to the documentation that came with your wireless device.

There are several site scan issues you should be aware of:

- More than one wireless network may appear in the list. These are other wireless networks that are within range of your network. Your neighbors, for instance, may be within range of your network. Each wireless network has a channel associated with it. We recommend there be at least a five-channel difference between your network and those of your neighbors. Having less than a five-channel difference may result in interference with your connection. By default, the Modem/Router uses channel 10. If you need to change this channel, you must do so using the **Wireless Setup** page of the **Zoom Configuration Manager**. For instructions on how to log in to the **Zoom Configuration Manager**, see page 10. After logging in, select **Wireless** from the left-hand menu. On the **Wireless** page you can select a new channel from the drop-down menu.
- 2 Test your wireless connections. From each computer or device that you set up, open your Web browser (for instance, Internet Explorer, Firefox, or Chrome) and try to connect to a familiar Web address.

If you connect successfully, you are ready to browse the Web!

To disconnect from the current network:

- 1 On your wireless device or computer, find the wireless network connection option (similar to the process of adding your device or computer to the network).
- 2 Click or highlight **Zoom_xxxxxx**, where xxxxxx are 6 random alphanumeric characters.
- 3 Select or click on **Disconnect** or similarly-named button.

Connecting a Computer with a Wireless adapter to the Modem/Router

- 1 Go to the computer that is set up with a wireless adapter that you want to add to the network. The computer should have software that will let it perform a **site search** to scan for available wireless networks in your area. When the Wireless Network Name (SSID) that you set in step 4 of the Setup Wizard of your Modem/Router's wireless network appears in the list select it as the network you want to use to connect to the Internet. If you did not change the Network ID (SSID), select the default name **Zoom_XXXXXX**. Where XXXXXX are 6 random alphanumeric characters. The complete Network ID is printed on the bottom label of your unit.

Tip!

For most wireless adapters, you will use its wireless configuration manager software and click a Scan button or select a Site Scan, Scan Networks, or other similarly named tab to do a site search. If you need help, refer to the documentation that came with your wireless adapter.

- 2 When prompted, enter the **Security Key** found on the bottom label of your unit. If you changed the key in Step 4 of the Setup Wizard, enter the new security key.
There are several site scan issues you should be aware of:
 - If you are trying to connect to a wireless network that already has security enabled, your wireless adapter might not recognize what type of security is on the network. You may need to manually set up the security for your adapter. If you need help, refer to the documentation that came with your wireless adapter.
 - **Windows 7, XP, and Vista users:** If you installed a wireless adapter on a Windows 7, XP, or Vista computer, Windows may try to automatically configure the adapter (rather than let you use the software provided with the wireless adapter). You will know this is happening because you will be prompted with a message about one or more wireless networks being available. You will also be able to click a link to open the **Wireless Network Connection Properties** dialog box. If this happens, click the link, clear the **Use Windows to configure my wireless network settings** check box, and then click **OK**. You can then use the software provided with your wireless adapter without interruption from Windows.
 - More than one wireless network may appear in the list. These are other wireless networks that are within range of your network. Your neighbors, for instance, may be within range of your network. Each wireless network has a channel associated with it. We recommend there be at least a five-channel difference between your network and those of your neighbors. Having less than a five-channel difference may result in interference with your connection. By default, the Modem/Router uses channel 10. If you need to change this channel, you must do so using the **Wireless Setup** page of the **Zoom Configuration Manager**. For instructions on how to log in to the **Zoom Configuration Manager**, see page 10. After logging in, select **Wireless** from the left-hand menu. On the **Wireless** page you can select a new channel from the drop-down menu.

- 2 Test your wireless connections. From each desktop or notebook computer that you set up, open your Web browser (for instance, Internet Explorer or Firefox) and try to connect to a familiar Web address.

If you connect successfully, you are ready to browse the Web!

To disconnect from the current network:

- 1 On your computer that has a wireless adapter, find the wireless network connection option (similar to the process of adding your computer to the network).
- 2 Click or highlight the Modem/Router's Wireless Network Name.
- 3 Select or click on **Disconnect** or similarly-named button.

Setting up your Network using WPS

If all the wireless devices you plan to connect to your network support **Wi-Fi Protected Setup (WPS)**, you can use WPS to connect and secure your devices in one step. To use WPS follow the instructions below.

Note: WPS configures one client device at a time. Please repeat the configuration method for each client on your wireless network that supports WPS security.

Configuration Methods

WPS offers three configuration methods. Choose the method that is compatible with the hardware and software options available on your "client device," which is the device you're connecting wirelessly to the Modem/Router.

Method One

Use this method if your client device has a **WPS** button. This button can be either a physical button on the unit or a software button in its application.

- 1 Press the **WPS** button on your Modem/Router and hold it in for seven (7) seconds until the Wireless LED starts blinking rapidly.

Important! The **Registrar** (the device configuring the WLAN) goes into the WPS mode and the **Enrollee** (the device joining the WLAN) then looks for it. You should always start the **Registrar** first. By default your Modem/Router is configured as a **Registrar**.

- 2 Click or press the **WPS** button on the client device.
- 3 Refer to your client device's documentation for further instructions, if necessary.

Method Two

Use this method if your client device already has a WPS PIN number. The client is the **Enrollee**.

- 4 If you haven't already done so, open a Web browser and type **http://192.168.2.1** in the address bar.

- a When the Configuration Manager launches, log in as admin, then select **Advanced > Basic Settings > Wireless** to open the Wireless Setup page.
 - b Click the **WPS Setup** button to open the **Wi-Fi Protected Setup** page.
 - c Select **PIN Code** from the **Config method** dropdown menu.
 - d Enter the **PIN number** from your client device.
 - e Click **Trigger** to start the connection process on the Modem/Router.
- Important!** You must do this within two minutes after starting the Modem/Router.
- f On the Modem/Router, when the program displays a message that the process succeeded, click **Save** to save the configuration

Method Three

Use this method if your client device requests the Modem/Router's PIN number. The client is the **Registrar**. Use this method if the client(s) are to connect to multiple access points so that a client will control the configuration instead of the Modem/Router.

- 1 If you haven't already done so, open a Web browser and type **http://192.168.2.1** in the address bar.
 - a When the Configuration Manager launches, log in as admin, then select **Advanced > Basic Settings > Wireless** to open the Wireless Setup page.
 - b Click the **WPS Setup** button.
 - c Select **Enrollee** from the **Config Mode** dropdown menu.
 - d Click **Generate Pin** to generate a new Pin number.
 - e Enter the Modem/Router's **Pin Number** into your client device. Refer to your client's documentation for further details.
- Important!** You must do this within two minutes after starting the Modem/Router.
- f Click **Trigger** to start the connection process on the Modem/Router.
 - g On the Modem/Router, when the program displays a message that the process succeeded, click **SET** to keep the Modem/Router from receiving new configuration parameters from another WPS Registrar.
 - h Click **Save** to save the configuration.

5

Understanding your Modem/Router's Voice Features

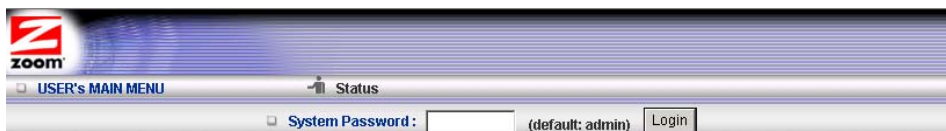
Most users will just plug their home phone or cordless base station into the Modem/Router's phone port and begin placing calls over the cellular voice network. This chapter is only for users who want to monitor their incoming, outgoing or missed calls, to setup call waiting or speed dialing, or to setup advanced telephony features.

If you are using the Modem/Router's built-in 3G+ modem to make voice calls and are connected to the Modem/Router through your computer's Ethernet port, you can go right ahead and log into the configuration manager. If you are using a wireless connection to access the Modem/Router you must first establish the wireless connection. If you are unsure how to set up a wireless connection see [Establishing your Wireless Network](#) on page 28.

- 1 Turn on your computer and Modem/Router, then launch the computer's Web browser.
- 2 In the Web browser address bar, type the Modem/Router's default IP address, **http://192.168.2.1** and then click **Enter**.

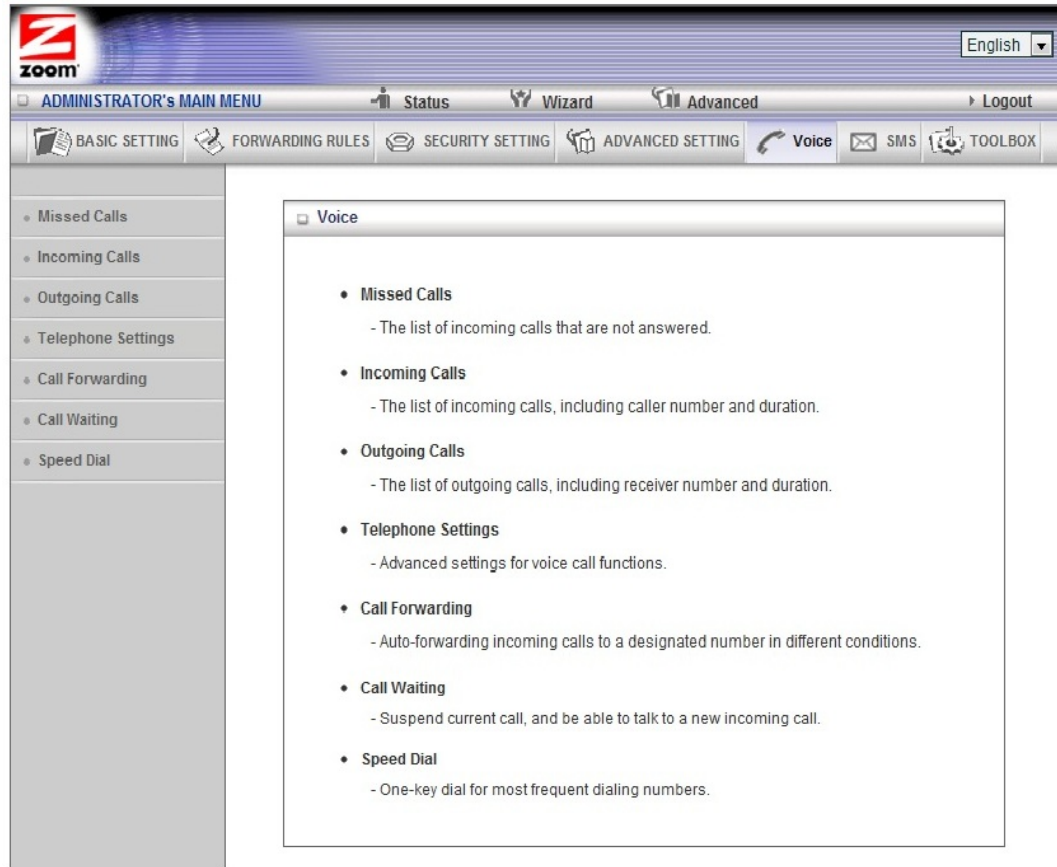
When the **MAIN MENU** opens for the first time, it displays a **System Status** page that summarizes the current settings and values for your system.

- 3 On the Toolbar, type **admin** (the default password) in the **System Password** field, then click **Login**.



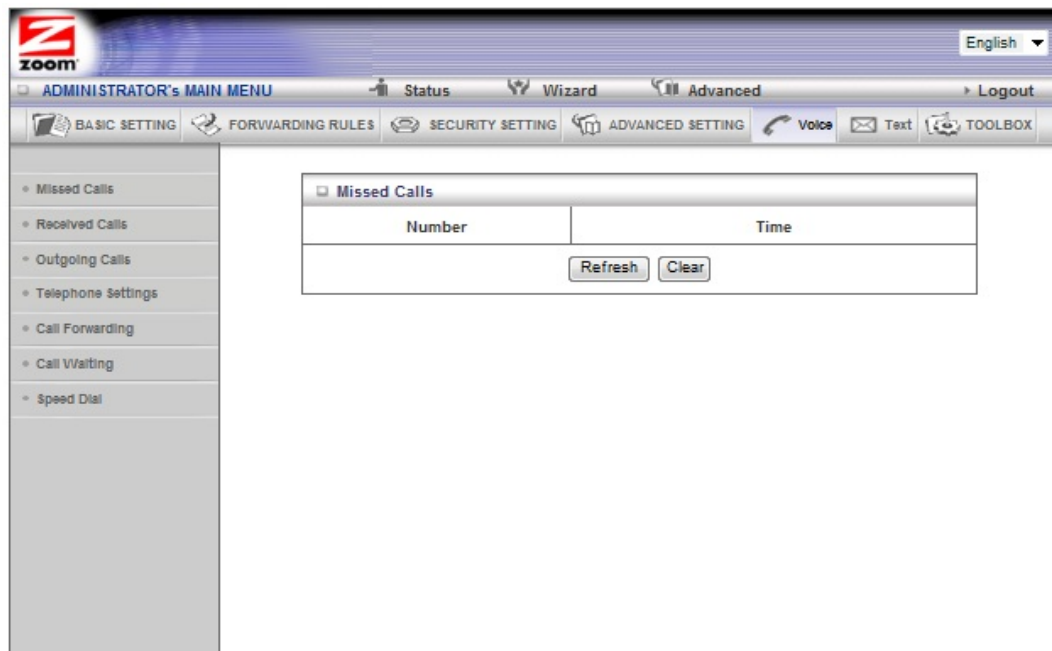
Note: if you have changed the **System Password**, you will use the new password to log in.

- 4 When you log in, the Configuration Manager opens its **Main Menu**. Select **Voice** on the top menu.



Missed Calls

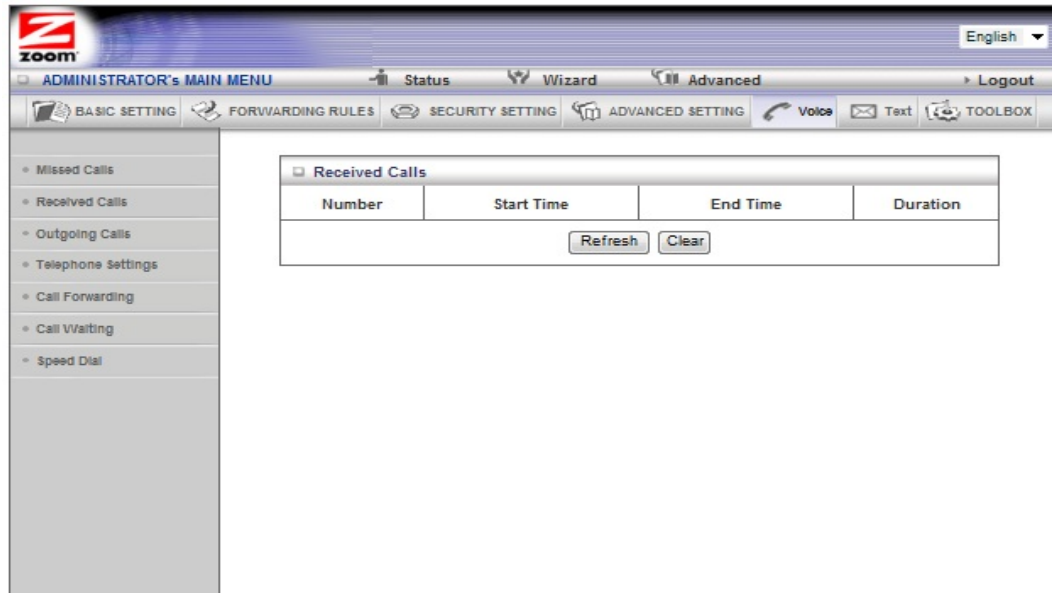
When you click on **Missed Calls** on the left hand menu, the following screen appears:



This page displays the calls that you missed. Clicking on **Refresh** updates the screen and clicking on **Clear** erases the existing missed calls.

Received Calls

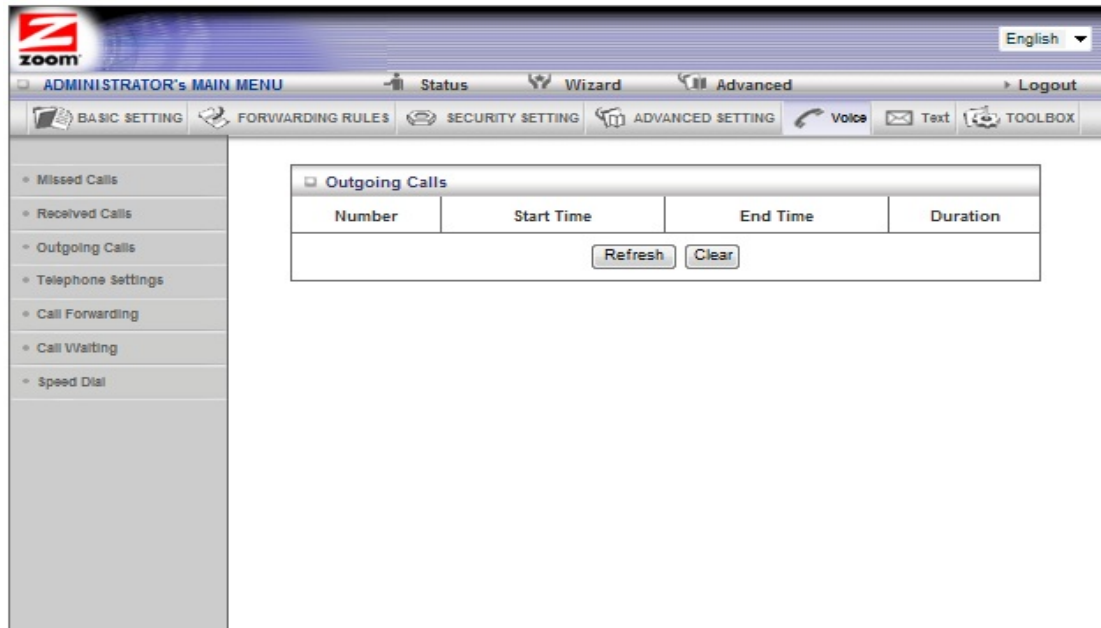
When you click on **Received Calls** on the left hand menu, the following screen appears:



This page displays the calls that you received including the number that called, the starting and ending time of the call, and the call duration. Clicking on **Refresh** updates the screen and clicking on **Clear** erases the existing received calls.

Outgoing Calls

When you click on **Outgoing Calls** on the left hand menu, the following screen appears:



This page displays the calls that you made including the number that you called, the starting and ending time of the call, and the call duration. Clicking on **Refresh** updates the screen and clicking on **Clear** erases the existing outgoing calls.

Telephone Settings

When you click on **Telephone Settings** on the left hand menu, the following screen appears:

The screenshot shows the Zoom Modem/Router web interface. At the top is the Zoom logo and a language dropdown set to 'English'. Below this is the 'ADMINISTRATOR'S MAIN MENU' with tabs for Status, Wizard, and Advanced, and a Logout link. A secondary menu bar contains icons and labels for BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING, Voice, Text, and TOOLBOX. On the left is a sidebar menu with options: Missed Calls, Received Calls, Outgoing Calls, Telephone Settings (selected), Call Forwarding, Call Waiting, and Speed Dial. The main content area is titled 'Telephone Settings' and contains a table with two columns: 'Item' and 'Setting'.

Item	Setting
▶ Caller ID	FSK ▼
▶ Dialing timeout	3 (Seconds)
▶ Use # to end dialing	<input type="checkbox"/> Enable
▶ Call log	<input type="checkbox"/> Enable

At the bottom of the table are 'Save' and 'Undo' buttons.

Caller ID

Your Modem/Router supports both **FSK** and **DTMF** Caller ID. If you are not receiving caller ID on your phone, try changing the setting.

Dialing Timeout

This is how long the Modem/Router will wait after you press a digit before it starts to dial.

Use # to end dialing

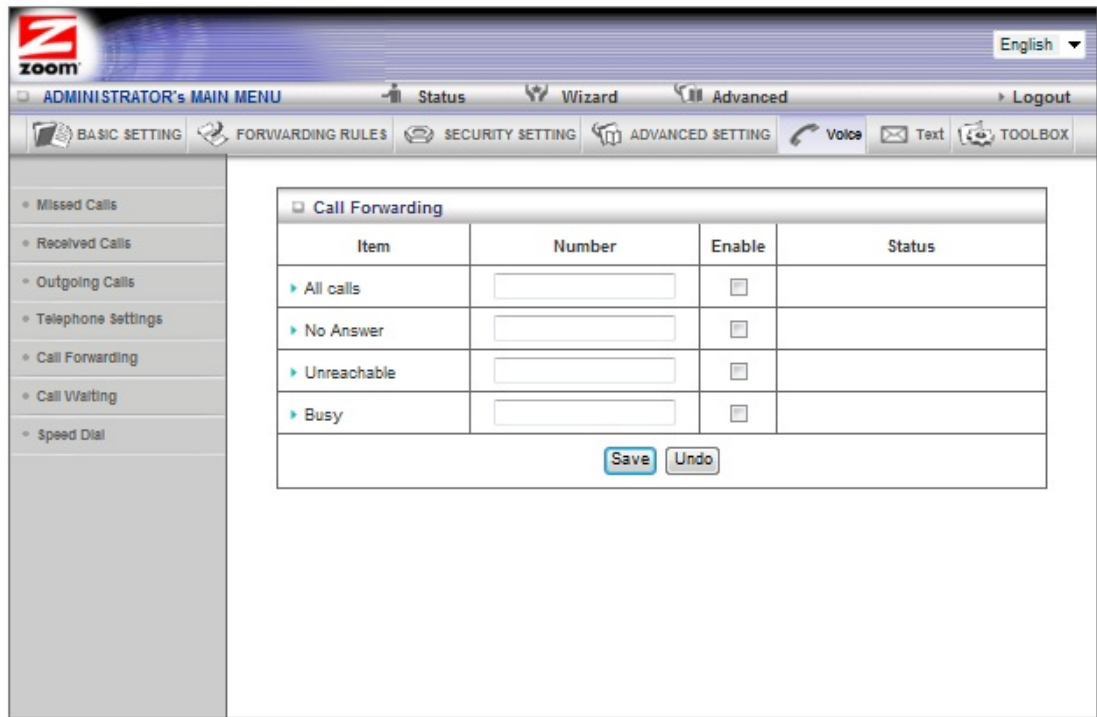
If you enter the # sign at the end of the phone number you are dialing, the Modem/Router will immediately dial the phone number and not wait for the **Dialing Timeout** to expire.

Call Log

When the Call log is enabled, all your Missed, Received, and Outgoing calls are logged by the Modem/Router.

Call Forwarding

When you click on **Call Forwarding** on the left hand menu, the following screen appears:



The screenshot shows the Zoom Administrator's Main Menu. The top navigation bar includes the Zoom logo, a language dropdown set to 'English', and links for 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', 'Voice', 'Text', and 'TOOLBOX'. The left sidebar lists various settings: 'Missed Calls', 'Received Calls', 'Outgoing Calls', 'Telephone Settings', 'Call Forwarding' (selected), 'Call Waiting', and 'Speed Dial'. The main content area is titled 'Call Forwarding' and contains a table with four columns: 'Item', 'Number', 'Enable', and 'Status'. The table has four rows: 'All calls', 'No Answer', 'Unreachable', and 'Busy'. Each row has an input field for the 'Number' and a checkbox for 'Enable'. Below the table are 'Save' and 'Undo' buttons.

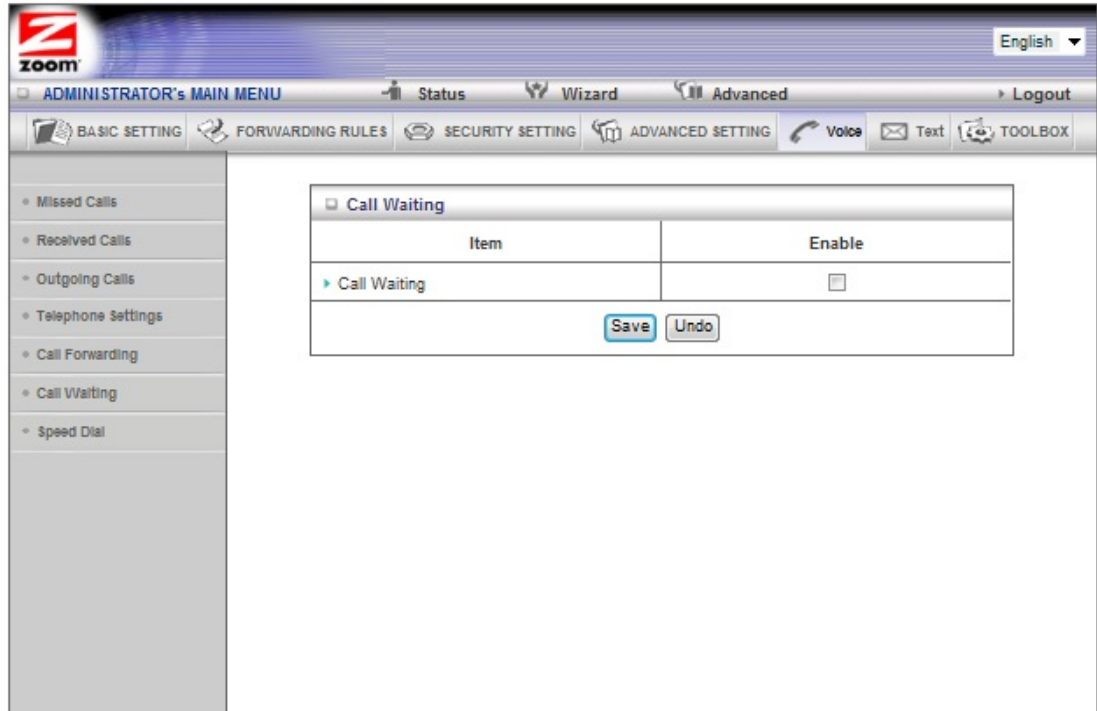
Item	Number	Enable	Status
▶ All calls	<input type="text"/>	<input type="checkbox"/>	
▶ No Answer	<input type="text"/>	<input type="checkbox"/>	
▶ Unreachable	<input type="text"/>	<input type="checkbox"/>	
▶ Busy	<input type="text"/>	<input type="checkbox"/>	

On this page you can forward your phone calls to a different number. You have the option of forwarding all calls or instead forwarding calls where there is No Answer, you are Unreachable, or your line is Busy. Enter the **Number** for the phone that should receive the forwarded call and click the **Enable box**. Click **Save** to store your settings.

Note: Call Forwarding must be supported and enabled by your service provider. If your service provider supports call forwarding and you have enabled it on the Modem/Router the **Status** field will say **Activated**.

Call Waiting

When you click on **Call Waiting** on the left hand menu, the following screen appears:



The screenshot shows the Zoom VoIP Administrator's Main Menu. The top navigation bar includes the Zoom logo, a language dropdown set to 'English', and links for 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', 'Voice', 'Text', and 'TOOLBOX'. The left sidebar lists various call management options: Missed Calls, Received Calls, Outgoing Calls, Telephone Settings, Call Forwarding, Call Waiting (highlighted), and Speed Dial. The main content area displays the 'Call Waiting' configuration page, which contains a table with two columns: 'Item' and 'Enable'. The table lists 'Call Waiting' with an unchecked checkbox in the 'Enable' column. Below the table are 'Save' and 'Undo' buttons.

Item	Enable
Call Waiting	<input type="checkbox"/>

Save Undo

Click the **Enable** checkbox to enable Call Waiting. If you receive a voice call while you are on another call will receive a beep indicating that there is another call present. Press down on the flash hook of your phone to transfer over to the new call. When you are done with that call press the flash hook again to transfer back to your original call.

Speed Dial

When you click on **Speed Dial** on the left hand menu, the following screen appears:

Number	Telephone Number	Enable
0	<input type="text"/>	<input type="checkbox"/>
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/>

To use **Speed Dial** enter the phone number that you want to speed dial in the **Telephone Number** field and check the box to enable it. For example, enter 555 5551515 in the **Telephone Number** field next to the number 1 and click **Save**. On your handset press the 1 key. The Modem/Router will automatically speed dial the stored number 555 5551515. Remember, by default the Modem/Router waits 3 seconds before dialing a phone number. You may want to enable the **Use # to end dialing** command to eliminate this wait time. See [Use # to end dialing](#) for more information.

6

Working with Text Messages

Your 3G+ Modem/Router with Wireless-N and Phone Port can be used to send and receive text messages. This chapter shows you how to use your Modem/Router to send a text message and how to manage your received text messages. This chapter also describes how you can send text messages to your 3G+ Modem/Router's to check its status and to control its Internet connection.

Using your Modem/Router to Send Text Messages

If you want to use the Modem/Router's built-in 3G+ modem to send text messages and you are connected to the Modem/Router through your computer's Ethernet port, you can go right ahead and log into the configuration manager. If you are using a wireless connection to access the Modem/Router, you must first establish the wireless connection. If you are unsure how to set up a wireless connection, see [Establishing your Wireless Network](#) on page 28.

- 1 Turn on your computer and Modem/Router, then launch the computer's Web browser.
- 2 In the Web browser address bar, type the Modem/Router's default IP address, **http://192.168.2.1** and then click **Enter**.

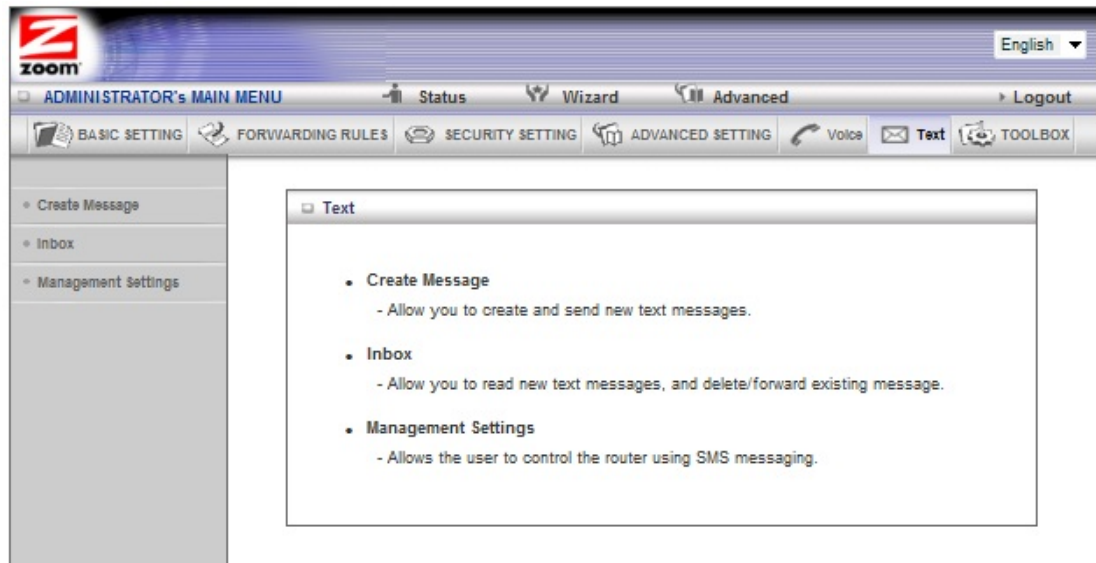
When the **MAIN MENU** opens for the first time, it displays a **System Status** page that summarizes the current settings and values for your system.

- 3 On the Toolbar, type **admin** (the default password) in the **System Password** field, then click **Login**.



Note: If you have changed the **System Password**, you will use the new password to log in.

- 4 When you log in, the Configuration Manager opens its **Main Menu**. Select **Text** on the top menu.



- 5 To send a message, select **Create Message** from the left hand menu. The following page appears:

The screenshot shows the 'Create Message' form. The left sidebar is the same as the previous screenshot. The main content area is titled 'Create Message' and contains a table with two columns: 'Item' and 'Setting'.

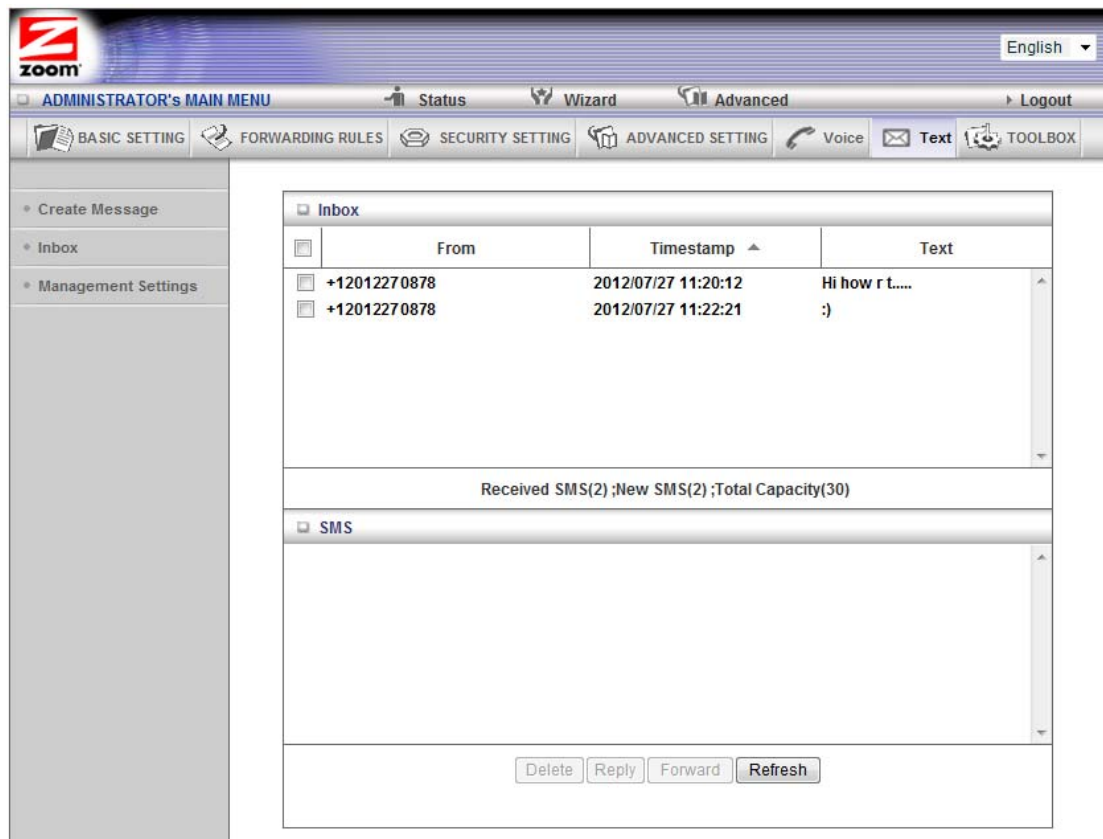
Item	Setting
Text message :	<div style="border: 1px solid gray; height: 80px; width: 100%;"></div> <p>Current text length : 0 . The max. length of a message is 160 characters.</p>
Phone Number :	<input type="text"/> <p>Add '+' for international calls.</p>

At the bottom of the form are two buttons: **Send** and **Cancel**.

- 6 Enter the message you want to send in the box next to **Text message**. The maximum length of the text message is 160 characters.
- 7 Enter the phone number of the person you want to send the text to in the **Phone number** box.
- 8 Click **Send** to send your text message. The Modem/Router will respond with a **Sent OK** message to let you know the message was sent.

Working with your Inbox

The Modem/Router will store incoming text messages on your SIM card. From your Inbox you can read, delete, reply, and forward text messages. To access your Inbox, click on Inbox from the left hand menu. The following page appears:



To read a text message, click on the message you want to view. The text message will now appear in the box at the bottom of the screen.

To reply to a text message, click on the checkbox next to the message and then click on **Reply**. Type your message and click **Send** to send it. To return to the Inbox, click on **Inbox** on the left hand menu

To forward a text message, click on the checkbox next to the message then click on **Forward**. Type your message and enter the phone number of the person you want to forward it to in the **Phone number** box. Click **Send** to send it. To return to the Inbox, click on **Inbox** on the left hand menu.

To delete a text message, click on the checkbox next to the message then click on **Delete**. The message will be deleted from your Inbox.

The Management Settings Page

When you click on **Management Settings**, the following page appears:

Management Settings

Item	Setting
Remote Management via SMS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Delete All Received SMS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Delete SMS for Remote Management	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Security Key	<input type="text"/>

Command Settings

Item	Setting
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Connect	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Disconnect	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Reconnect	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Reboot	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Notification Settings

Item	Setting
WAN Link Up	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WAN Link Down	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Secondary WAN Link is Up	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Secondary WAN Link is Down	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Access Control List

Item	Setting
Access Control	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Any Phone Number	<input type="checkbox"/> Management
Phone 1 <input type="text"/>	<input type="checkbox"/> Management <input type="checkbox"/> Notification
Phone 2 <input type="text"/>	<input type="checkbox"/> Management <input type="checkbox"/> Notification
Phone 3 <input type="text"/>	<input type="checkbox"/> Management <input type="checkbox"/> Notification
Phone 4 <input type="text"/>	<input type="checkbox"/> Management <input type="checkbox"/> Notification
Phone 5 <input type="text"/>	<input type="checkbox"/> Management <input type="checkbox"/> Notification

Your Modem/Router can be controlled remotely by text messages that approved senders can send to your modem/router's phone number, which is the same phone number you use when you want to receive voice calls. If an approved user has the

correct password, that user can check the Internet connection status, connect to the Internet, disconnect from the Internet, or reboot the Modem/Router.

Management Settings

These commands control how the Modem/Router handles SMS (text-messaging) commands.

Remote Management via SMS

Click **Enable** to enable remote control of your Modem/Router using Text messaging by someone with the right Security Key as discussed below.

Delete All Received SMS

Click **Enable** to delete all received text messages, including messages already stored in your SIM card and messages received in the future. This affects both regular text messages and remote management text messages. If you do not want to store received text messages on your SIM card, you should enable this feature.

Your SIM card is typically limited to storing 30 messages. Once you reach this limit no further messages will be received. To avoid this limitation all received messages can be deleted.

Delete SMS for Remote Management

Click **Enable** to delete all received remote management text messages, including messages already stored in your SIM card and messages received in the future. This does not affect regular text messages sent to your Modem/Router's phone number.

Security Key

If you enable remote management, you must enter a **Security Key**. This key gives a user access to the system. This key can be 1 to 32 alphanumeric characters. When you send a command through text messaging to the modem, you will need to include this key. There should be a space between the security key and the command you are sending. For example if you want to send the **Reboot** command to your Modem/Router, send the following SMS message:

<security key> reboot

Command Settings

You can control your Modem/Router remotely by sending a command using SMS (text messaging) to the phone number of the modem/router. The Modem/Router must be enabled for the command first, as discussed below.

Status

Click **Enable** if you want to be able to check the status of your

Modem/Router by using this text message:

<security key> status

The Modem/Router responds with the WAN IP, Carrier Name, the type of network (HSPA+, HSUPA, WCDMA, GPRS), and the amount of time your Modem/Router's Internet connection has been active.

Connect

Click **Enable** if you want to be able to remotely ask your Modem/Router to make an Internet connection by using this text message:

<security key> connect

If your Internet connection is down, you can send the Connect text message to re-establish the connection. If your Internet connection is up, the Connect text message won't affect the Internet connection.

Disconnect

Click **Enable** if you want to be able to remotely force your Modem/Router to disconnect from the Internet by using this text message:

<security key> disconnect

If the Modem/Router receives a Disconnect message, it will **not** try to re-connect if the WAN is set to auto-reconnect.

Reconnect

Click **Enable** if you want to be able to remotely reconnect your Internet connection by using this text message:

<security key> reconnect

Reconnect will disconnect the current Internet connection and then start a new connection.

Reboot

Click **Enable** if you want to be able to reboot your Modem/Router remotely by using this text message:

<security key> reboot

Notification Settings

These settings allow you to select which notifications get sent out to phone numbers on your Access Control list, a list of phone numbers for people allowed to send or receive text messages relating to your Modem/Router. These messages are only sent out if you have **Access Control** enabled for at least one phone number that's set up for notification. See [Access Control List](#) below for more information.

WAN Link Up

Click **Enable** if you want the Modem/Router to send a notification message to users in the access control list when an Internet connection is first established.

WAN Link Down

Click **Enable** if you want the Modem/Router to send a notification message to users in the access control list when the Internet connection goes down.

Secondary WAN is Up

Click **Enable** if you want the Modem/Router to send a notification message to users in the access control list that the secondary Internet connection has been established.

Secondary WAN is Down

Click **Enable** if you want the Modem/Router to send a notification message to users in the access control list that the secondary Internet connection goes down.

Access Control List

These commands allow you to specify what phone numbers can send commands to your Modem/Router and what phone numbers the Modem/Router will send notifications to. If you have Remote Management enabled and Access Control disabled, then any phone number can send commands to the Modem/Router if it has the correct Security Key.

Access Control

Click **Enable** if you want to control what phone numbers can send commands to the Modem/Router. If you want to send notifications out when your connection goes down, for example, then you must enable **Access Control** and have at least one phone number set up for notifications.

Any Phone Number

Click **Enable** if you want the Modem/Router to allow any phone number to send commands to the Modem/Router. This command is used if you decide to enable notifications but still want any phone number that enters the correct security key to be able to control the Modem/Router.

Phone 1-5

Enter the phone numbers you want to either control the Modem/Router and/or receive notifications. If you want the phone number to receive notifications of events such as the Modem/Router disconnected, check the **Notifications** box. If you want only the phone numbers you list to be able to control the Modem/Router, check the **Management** box. If you only want certain phone numbers to be able to control the Modem/Router, do not enable **Any Phone Number**.

Example

This example will show you how to set up and send a command to the Modem/Router.

- 1 On the **Management Settings** page, click **Enable** next to **Remote Management via SMS** comment to enable remote management of your Modem/Router.
- 2 Enter a **Security Key** to control access to the Modem/Router. For example enter JIM123 in the **Security Key** textbox.
- 3 Next, select which commands you wish to enable. For example if you want to be able to check the status and reboot the Modem/Router remotely, click **Enable** next to the **Status** and **Reboot** command.
- 4 Click **Save**. After the Modem/Router saves the changes, click **Reboot** to make the changes active.

The Modem/Router is now set up to receive the **Status** and **Reboot** command from any phone number that enters the correct **Security Key** JIM123. To test your setup, send a text message to the Modem/Router in this format.

JIM123 status

You will receive an SMS message back with the status of your Modem/Router. This message will be in the following format:

WAN IP [xxx.xxx.xxx.xxx]

Network [AT&T]

Type [HSUPA]

Conn Time [03:45:20]

7

Using the Configuration Manager's Advanced Program

*Most users will not need to manually set up their Modem/Router. In the unlikely event that you do, you can use the Configuration Manager's **Advanced** program to change the Modem/Router's default settings.*

This chapter includes:

- Suggestions for settings that you might want to change
- A brief description of the online and context-sensitive help that is available
- Instructions for launching the **Advanced** program
- An overview of the available configuration menus and settings

Changing Default Settings

Here are some reasons why you might want to use the **Advanced** program to change the Modem/Router's default settings.

- You need to manually enter your service provider settings for the built-in 3G+ modem.
- You want to connect the Modem/Router to your ADSL or cable modem, using the built-in 3G+ modem as a backup Internet connection. See [The Basic Setup Page](#) on page 55 for details.
- You want to block access to certain URLs or set up Scheduling usage rules. See [The URL Blocking Page](#) on page 71 and [The Schedule Rule and Schedule Rule Setting Pages](#) on page 82 for details.
- You want to hide the SSID name so other network users cannot see your wireless network. See [The Wireless Setting Page](#) on page 59 for details.
- You want to change Modem/Router settings to establish a firewall to guard against unauthorized access to your network. See [The MAC Address Control Page](#) on page 73 for details.
- You want to set up a Virtual Server or DMZ so that your games or gaming consoles can access the Internet through your Modem/Router's firewall. See [Configuring Forwarding Rules](#) on page 64 for details.

- You want your Mobile Broadband connection to be terminated by the Modem/Router if you haven't used the Internet for a specified period of time. The default setting is **Auto Reconnect (always on)**. See [The Basic Setup Page \(Connection Control\)](#) on page 55 for details.
- You want to change the default wireless security on your Modem/Router. See [Wireless Settings](#) on page 59 for details.
- You want to back up Modem/Router settings that you made using the Configuration Manager. See [The Backup Setting Dialog](#) on page 87 for details.

Online Help

The **Advanced** program provides both online and context-sensitive help that guides you in changing the settings on each menu.

- To access **online help**, click **[HELP]** on the menu's Toolbar. Each **[HELP]** page describes the fields on the active page and, when applicable, the required or recommended entries.
- The **context-sensitive help** automatically displays a question mark to the right of the cursor, then opens a message box in the left pane of the page. The message box contains text that describes the active field and its required or recommended entry.

Launching the Configuration Manager's Advanced Program

If you are connected to the Modem/Router through your computer's Ethernet port, you can go right ahead and log into the configuration manager. If you are using a wireless connection to access the Modem/Router, you must first set up the wireless connection. If you are unsure how to set up a wireless connection see [Establishing your Wireless Network](#) on page 28. Turn on your computer and Modem/Router, then launch your Web browser.

- 5 In the Web browser address bar, type the Modem/Router's default IP address, **http://192.168.2.1** and then click **Enter** to launch the Configuration Manager.

When the Configuration Manager's **MAIN MENU** opens, it displays a **Status** page that summarizes the basic settings and current values for your setup.

- 6 On the Toolbar, type **admin** (the default password) in the **System Password** field, then click **Login**.



Note: If you have changed the **System Password**, you will use the new password to log in.

- 7 Click **Advanced** on the Toolbar to launch the **Advanced** program.

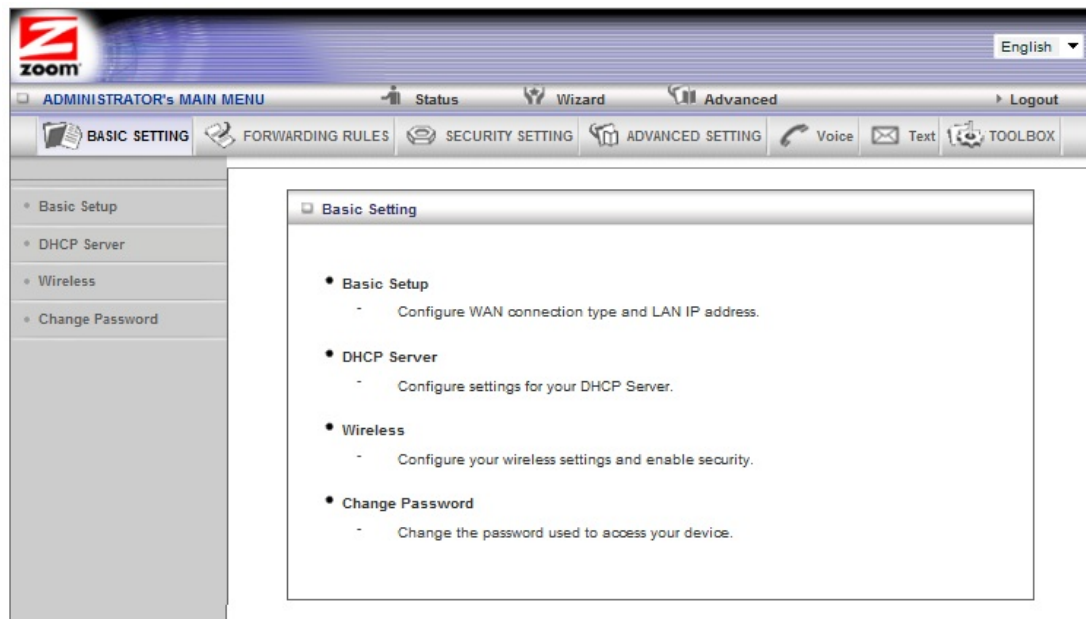


- 8 On the **Basic Settings** page, click one of the Toolbar buttons (**Basic Settings**, **Forwarding Rules**, **Security Settings**, **Advanced Settings**, or **Toolbox**).

The corresponding window opens. Each window contains a description of the configuration options at center and a configuration menu on the left pane.

Configuring Basic Settings

The **Basic Settings** page lists the four configuration menus on the left pane and provides a description of the configuration menus at center.



The Basic Setup Page

You can use the **Basic Setup** page to configure your LAN and WAN setup.

Note: The following image depicts the fields that the program displays when 3G+ is selected as the **WAN Type**. The fields will differ for each **WAN Type**. See the online help for a description of each **WAN Type** and its corresponding fields. If you want to use the built-in 3G+ modem as a backup to your cable or ADSL modem, go to [Using the 3G+ modem as a backup](#) on page 57.

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING Voice Text TOOLBOX																																																	
<ul style="list-style-type: none"> Basic Setup DHCP Server Wireless Change Password 	<div> <div>Basic Setup [HELP]</div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>▶ LAN IP Address</td> <td>192.168.2.1</td> </tr> <tr> <td>▶ 3G Failover</td> <td> <input type="checkbox"/> Check for Wan Connection Internet host: <input type="text"/> </td> </tr> <tr> <td>▶ WAN Type</td> <td>3G+ ▼</td> </tr> <tr> <td>▶ Profile</td> <td> <input type="radio"/> Auto-Detection <input checked="" type="radio"/> Manual </td> </tr> <tr> <td>▶ Country</td> <td>USA ▼</td> </tr> <tr> <td>▶ Providers</td> <td>AT&T (Non-contract)(voice/data) ▼</td> </tr> <tr> <td>▶ 3G Network</td> <td>WCDMA/HSPA ▼</td> </tr> <tr> <td>▶ APN (Not required by all providers)</td> <td>WAP.CINGULAR</td> </tr> <tr> <td>▶ PIN Code</td> <td><input type="text"/></td> </tr> <tr> <td>▶ Dialed Number</td> <td>*99#</td> </tr> <tr> <td>▶ Username</td> <td>WAP@CINGULARS.COM</td> </tr> <tr> <td>▶ Password</td> <td>*****</td> </tr> <tr> <td>▶ Authentication</td> <td> <input checked="" type="radio"/> Auto <input type="radio"/> PAP <input type="radio"/> CHAP </td> </tr> <tr> <td>▶ Primary DNS</td> <td><input type="text"/></td> </tr> <tr> <td>▶ Secondary DNS</td> <td><input type="text"/></td> </tr> <tr> <td>▶ Prefer Service Mode</td> <td>Auto Mode ▼</td> </tr> <tr> <td>▶ Connection Control</td> <td>Auto Reconnect (always-on) ▼</td> </tr> <tr> <td>▶ Maximum Idle Time</td> <td>0 seconds</td> </tr> <tr> <td>▶ Allowed Connection Time</td> <td> <input checked="" type="radio"/> Always <input type="radio"/> By Schedule </td> </tr> <tr> <td>▶ Keep Alive</td> <td> <input checked="" type="radio"/> Disable <input type="radio"/> Use LCP Echo Request ▶ lcp-echo-interval: 10 seconds ▶ lcp-echo-failure: 3 times </td> </tr> <tr> <td>▶ Roaming</td> <td><input type="checkbox"/> Enable</td> </tr> <tr> <td>▶ MTU</td> <td>0 (0 is auto)</td> </tr> <tr> <td colspan="2"> <div>Save Undo</div> </td> </tr> </tbody> </table> </div>	Item	Setting	▶ LAN IP Address	192.168.2.1	▶ 3G Failover	<input type="checkbox"/> Check for Wan Connection Internet host: <input type="text"/>	▶ WAN Type	3G+ ▼	▶ Profile	<input type="radio"/> Auto-Detection <input checked="" type="radio"/> Manual	▶ Country	USA ▼	▶ Providers	AT&T (Non-contract)(voice/data) ▼	▶ 3G Network	WCDMA/HSPA ▼	▶ APN (Not required by all providers)	WAP.CINGULAR	▶ PIN Code	<input type="text"/>	▶ Dialed Number	*99#	▶ Username	WAP@CINGULARS.COM	▶ Password	*****	▶ Authentication	<input checked="" type="radio"/> Auto <input type="radio"/> PAP <input type="radio"/> CHAP	▶ Primary DNS	<input type="text"/>	▶ Secondary DNS	<input type="text"/>	▶ Prefer Service Mode	Auto Mode ▼	▶ Connection Control	Auto Reconnect (always-on) ▼	▶ Maximum Idle Time	0 seconds	▶ Allowed Connection Time	<input checked="" type="radio"/> Always <input type="radio"/> By Schedule	▶ Keep Alive	<input checked="" type="radio"/> Disable <input type="radio"/> Use LCP Echo Request ▶ lcp-echo-interval: 10 seconds ▶ lcp-echo-failure: 3 times	▶ Roaming	<input type="checkbox"/> Enable	▶ MTU	0 (0 is auto)	<div>Save Undo</div>	
Item	Setting																																																
▶ LAN IP Address	192.168.2.1																																																
▶ 3G Failover	<input type="checkbox"/> Check for Wan Connection Internet host: <input type="text"/>																																																
▶ WAN Type	3G+ ▼																																																
▶ Profile	<input type="radio"/> Auto-Detection <input checked="" type="radio"/> Manual																																																
▶ Country	USA ▼																																																
▶ Providers	AT&T (Non-contract)(voice/data) ▼																																																
▶ 3G Network	WCDMA/HSPA ▼																																																
▶ APN (Not required by all providers)	WAP.CINGULAR																																																
▶ PIN Code	<input type="text"/>																																																
▶ Dialed Number	*99#																																																
▶ Username	WAP@CINGULARS.COM																																																
▶ Password	*****																																																
▶ Authentication	<input checked="" type="radio"/> Auto <input type="radio"/> PAP <input type="radio"/> CHAP																																																
▶ Primary DNS	<input type="text"/>																																																
▶ Secondary DNS	<input type="text"/>																																																
▶ Prefer Service Mode	Auto Mode ▼																																																
▶ Connection Control	Auto Reconnect (always-on) ▼																																																
▶ Maximum Idle Time	0 seconds																																																
▶ Allowed Connection Time	<input checked="" type="radio"/> Always <input type="radio"/> By Schedule																																																
▶ Keep Alive	<input checked="" type="radio"/> Disable <input type="radio"/> Use LCP Echo Request ▶ lcp-echo-interval: 10 seconds ▶ lcp-echo-failure: 3 times																																																
▶ Roaming	<input type="checkbox"/> Enable																																																
▶ MTU	0 (0 is auto)																																																
<div>Save Undo</div>																																																	

WAN Type

Set to **3G+**, by default. You can choose another option from the dropdown menu, based on the WAN connection type that your service provider supports.

APN, PIN Code, Dialed Number, Username and Password

Identifiers assigned by some service providers, if needed. Contact your service provider if this information is missing or refer to [Appendix A Mobile Broadband Settings](#) for a list of settings for various providers.

Authentication

Set to **Auto**, by default. Optionally, click **Password Authentication Protocol (PAP)**, or **Challenge Handshake Authentication Protocol (CHAP)**, if supported by your service provider.

Primary DNS and Secondary DNS

Identifiers for the **Domain Name Servers**. These identifiers are provided by your service provider.

Connection Control

Specifies the method for connecting or disconnecting the WAN session based on network activity. **Auto Reconnect (always on)** is the default. Other options are **Connection-on-Demand** or **Manual**.

Maximum Idle Time

Specifies the duration (in seconds) of inactivity before the device disconnects. The default is **0**, which disables this feature.

Keep Alive

Disabled by default. Select **LCP Echo Request** to keep the connection alive.

Using your 3G+ modem as a Backup

You can use the built-in 3G+ modem to provide Internet access if your DSL or Cable service stops working. To setup 3G Failover first you need to setup the 3G+ modem and verify that it works then you setup your cable or DSL connection.

To set up the 3G Failover, follow the instructions below:

- 1 Run the **Setup Wizard**. On the **Select WAN Type** page choose the built-in mobile broadband modem as your WAN connection. See [Launching the Configuration Manager's Setup Wizard](#) on page 12.
- 2 Next you need to change the WAN connection to your cable or DSL modem. Run the **Setup Wizard** again this time selecting your Cable or DSL modem as your WAN connection type.
- 3 Once you have configured your Cable or DSL modem you need to enable **3G** Failover. To enable **3G Failover** select Basic Settings from the Configuration Manager's Advanced Page. See [Launching the Configuration Manager's Advanced Program](#) on page 54 if you don't know how to access the Advanced setting page.
- 4 On the Basic Setup page click the **Check the Wan Connection** checkbox.
- 5 Enter the Domain Name Server IP address that your Cable or ADSL modem uses in the **Internet host** textbox. This is the IP address that the Modem/Router will use to verify that your DSL or Cable connection is active. To get the IP address of your Domain Name server:
 - a Go to the **Status** page from the Zoom Configuration Manager. Locate the Domain Name Server.
 - b In the **WAN Status** column, copy one of the displayed IP addresses (either the primary or secondary DNS IP address).
 - c From the Configuration Manager, click on **Advanced** and

then **Basic Setup** and paste the IP address into the **Internet host** textbox.

6 Click **Save**.

The DHCP Server Page

You can use the **DHCP Server** page to configure your DHCP server. If you want to change the default values, please click **[HELP]**, which opens a page that describes each item and the recommended values.

The screenshot displays the Zoom DHCP Server configuration interface. The top navigation bar includes 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this, a secondary bar shows 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', 'Voice', 'Text', and 'TOOLBOX'. The left sidebar lists 'Basic Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'DHCP Server' and features a table with the following settings:

Item	Setting
DHCP Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IP Pool Starting Address	100
IP Pool Ending Address	200
Lease Time	86400 Seconds
Domain Name	

At the bottom of the table are buttons for 'Save', 'Undo', 'More>>', 'Clients List...', and 'Fixed Mapping...'. A '[HELP]' link is located in the top right corner of the table area.

The Wireless Setting Page

You can use the **Wireless Setting** page to configure your wireless LAN setup. By default your Modem/Router ships with wireless security enabled. The Wireless Network Name and Security Key for your unit is printed on the bottom case label.

The screenshot shows the 'Wireless Setting' page in the Zoom configuration manager. The page has a sidebar on the left with links to 'Basic Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main area contains a table with wireless settings. At the top of the main area is a 'ADMINISTRATOR'S MAIN MENU' bar with links to 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a 'BASIC SETTING' bar with links to 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', 'Voice', 'Text', and 'TOOLBOX'. The 'Wireless Setting' table has two columns: 'Item' and 'Setting'. The settings are: 'Wireless Function' (Enable/Disable), 'Wireless Schedule' ((0) Always), 'Wireless Network Name (SSID)' (Zoom_2848DD), 'SSID Broadcast' (Enable/Disable), 'Channel' (10), 'Wireless Mode' (B/G/N mixed), 'Authentication' (WPA-PSK / WPA2-PSK), '802.1X' (Enable/Disable), 'Encryption' (TKIP / AES), and 'Security Key' (aaba5ebee807a3). At the bottom of the table are buttons for 'Save', 'Undo', 'WDS Setting...', 'WPS Setup...', 'Wireless Client List...', and 'Wireless Advanced Setting'.

Item	Setting
Wireless Function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless Schedule	(0) Always
Wireless Network Name (SSID)	Zoom_2848DD
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	10
Wireless Mode	B/G/N mixed
Authentication	WPA-PSK / WPA2-PSK
802.1X	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Encryption	TKIP / AES
Security Key	aaba5ebee807a3

Wireless Function

Accept the default, **Enable**. Click the **Disable** checkbox only if you do not want wireless clients to access your network.

Wireless Schedule

If you want your wireless to be off at certain times you can set up a scheduling rule that controls when wireless is enabled. See [Scheduling Rules](#) for more information.

Wireless Network Name (SSID)

Refers to the **S**ervice **S**et **I**dentifier for your device. By default, the SSID for the Modem/Router with Wireless-N is **Zoom_xxxxxx**, where xxxxxx is six random alphanumeric characters. The Wireless Network Name of your device is found on the bottom label of your unit. You can change the SSID to a name of your choice. The wireless network name can be up to 32 alphanumeric characters. If you change the name, make sure that all devices on your network use the new SSID as the access point.

SSID Broadcast

To hide your network's SSID name, which disables automatic broadcasting

of the SSID and makes the wireless access point (your Modem/Router) invisible to wireless clients on the network, click the **Disable** radio button.

Channel

Refers to the wireless network channel assigned to your LAN. By default, the Modem/Router uses channel **10**.

Wireless Mode

Accept the default, **B/G/N mixed** if the client devices on your network use various wireless standards. Otherwise, select the wireless standard used by all wireless devices on your network. Having a single standard will speed up the wireless throughput.

Authentication

Select an **Authentication** method for all devices on your wireless network. If you are using gaming devices that require WEP, then you must configure all devices with this method. By default your Modem/Router is set for **WPA-PSK/WPA2-PSK**. A random **Security Key** is programmed in at the factory. The key can be found on the bottom label on your unit.

For **WPA-PSK/WPA2-PSK** Authentication:

You can select **WPA-PSK/WPA2 PSK** if your devices support both authentication methods. Optionally, select **WPA-PSK** or **WPA2-PSK** if all devices on your network support only one of these authentication methods.

For **WEP** Authentication:

If one of your devices uses WEP you should select **WEP-Auto**. If you know what type of WEP your device uses select either **WEP-Open** to use Open System authentication. Select **WEP-Shared** to use Shared Key authentication.

Encryption

Select an **Encryption** method that corresponds to the **Authentication** method that you chose.

If you chose a WPA-PSK/WPA2-PSK Authentication method:

Accept **TKIP/AES** encryption (the **WPA-PSK/WPA2-PSK** default), which supports dynamic encryption keys using TKIP or AES algorithms, or choose one of the other options.

Select **AES** if you chose **WPA2-PSK** for the authentication method.

Select **TKIP** if you chose **WPA-PSK** for the authentication method.

In the **Security Key** field, enter a minimum 8-character key.

If you chose a WEP Authentication method:

Select **WEP**.

Key Format

We recommend using Hex because not all Ascii keys are compatible. Hex keys use the numbers 0-9 and the letters A-F.

Encryption WEP Key 1, 2, 3, 4

If you selected Hex format and you chose a 128-bit key length, 26 hexadecimal values are required. Write the 26-hexadecimal key in the space below for future reference, and then enter it in the Key 1 box.

If you selected Hex format and you chose a 64-bit key length, 10 hexadecimal values are required. Write the 13-hexadecimal key in the space below for future reference, and then enter it in the Key 1 box.

If you selected ASCII format, and you chose a 128-bit key length, 10 ASCII characters are required. Write the 13-ASCII-character key in the space below for future reference, and then enter it in the Key 1 box.

If you selected ASCII format, and you chose a 64-bit key length, 5 ASCII characters are required. Write the 5-ASCII-character key in the space below for future reference, and then enter it in the Key 1 box.

Click **WPS Setup** to launch the **WiFi Protected Setup (WPS)** Setup program. For instructions, please refer to [WPS Configuration](#) on page 35.

We recommend you set WPA2/WPA security unless you know that you will be connecting devices to your network that support only WEP. If you know you have some devices that only support WEP, go to [WEP Configuration](#) on page 63. Otherwise, continue to **WPA2/WPA Configuration**.

WPA2/WPA Configuration

Wi-Fi Protected Access (WPA) is an encryption method that offers a stronger security standard than WEP.

Important! If you choose to configure your Modem/Router using either WPA2 or WPA encryption, then you must configure all devices on your wireless network with the same WPA encryption method and shared key.

You can configure WPA2 or WPA encryption using the [Wireless Setting Page](#) of the Configuration Manager's **Advanced** program.

The screenshot shows the 'Wireless Setting' page in the Zoom Administrator's Main Menu. The left sidebar lists 'Basic Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'Wireless Setting' and contains a table of settings.

Item	Setting
Wireless Function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless Schedule	(0) Always ▼
Wireless Network Name (SSID)	Zoom_2848DD
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	10 ▼
Wireless Mode	B/G/N mixed ▼
Authentication	WPA-PSK / WPA2-PSK ▼
802.1X	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Encryption	TKIP / AES ▼
Security Key	aaba5ebee807a3

At the bottom of the settings table, there are buttons for 'Save', 'Undo', and 'WDS Setting...'. Below these are three additional buttons: 'WPS Setup...', 'Wireless Client List...', and 'Wireless Advanced Setting'.

- 1 In the **Authentication** drop down bar select **WPA – PSK/WPA2 – PSK**. If you know all your devices support WPA2-PSK you can select it instead. This is the default setting.
- 2 In the **Security Key** field enter a value for the key. The maximum value is 42 characters. The minimum value is 8 characters. By default a **Security Key** is programmed into your unit at the factory. This Security Key is found on the bottom label of your unit. Most users should use this key.
- 3 If you change the **Security Key** write it down and put it where you can find it – on the bottom of the case, for instance.
- 4 Click **Save**. If you are connected wirelessly to the Modem/Router you will lose the connection as soon as you click **Save**. When you re-establish your wireless connection you will be prompted for the security key that you just entered. You must enter this key to be able to connect to the Modem/Router.
- 5 Now you need to set up each of your wireless devices with the Security Key that you entered. See [Establishing your Wireless Network](#) on page 28 for instructions on connecting devices to the Modem/Router.

WEP Configuration

Wired Equivalent Privacy (WEP) is a basic encryption method that does not offer the security strength of WPA or WPA2. Use this method only if some of your network's wireless devices, such as a gaming console, do not support WPA2/WPA.

Important! If you choose to configure your Modem/Router using WEP encryption, then you must configure all devices on your wireless network with the same WEP encryption method and key.

You can configure WEP encryption using the [Wireless Setting Page](#) of the Configuration Manager's **Advanced** program.

- 1 In the **Encryption** drop down bar select **WEP**.
- 2 In the WEP KEY 1 box you have the choice of entering either a 64-bit key or a 128-bit key. If you want to use a 64-bit key enter 10 hex characters. (Hex characters are the numbers 0-9, and the characters A-F.) If you want to use a 128-bit key enter 26 Hex characters. A 64-bit key provides slightly faster performance while a 128-bit key provides slightly better security. We recommend using a 64-bit key.
- 3 Write down this key and put it where you can find it – on the bottom of the Modem/Router case, for instance.
- 4 Click **Save**. If you are connected wirelessly to the Modem/Router you will lose the connection as soon as you click **Save**. When you re-establish your wireless connection you will be prompted for the key that you just entered. You must enter this key to be able to connect to the Modem/Router.
- 5 Now you need to set up each of your wireless devices with the Key that you entered. See [Establishing your Wireless Network](#) on page 28 for instructions on connecting devices to the Modem/Router.

The Change Password Page

You can use this page to change your login password. To view or change configuration settings, you must enter a password. Your Modem/Router has a default password (**admin**) that was set by the factory and that you used to access the **Configuration Manager** initially. To safeguard your configuration, particularly if you make changes, we recommend that you change the login password.

Item	Setting
Old Password	<input type="text"/>
New Password	<input type="text"/>
Retype Password	<input type="text"/>

Note: If you forget the new password, you won't have access to the Configuration Manager and will need to [restore the device to its factory settings](#) thus losing any changes you made to your Modem/Router's configuration. To avoid this problem, we recommend that you write the new password and save it in a convenient location.

Configuring Forwarding Rules

If you are using your Modem/Router for gaming, you may need to make changes to the Modem/Router's firewall setting for the game to work. This is done by setting up a DMZ or virtual server, or using port triggering so that the modem's firewall won't block the other players from your system during your gaming. The main difference between the three methods is the amount of access someone has to your system.

A virtual server will allow access to your computer or gaming station on certain ports. A port is a channel that is used by applications (such as games) for communication. For example, the directions for the game you want to play over the Internet might tell you to open up port 6000.

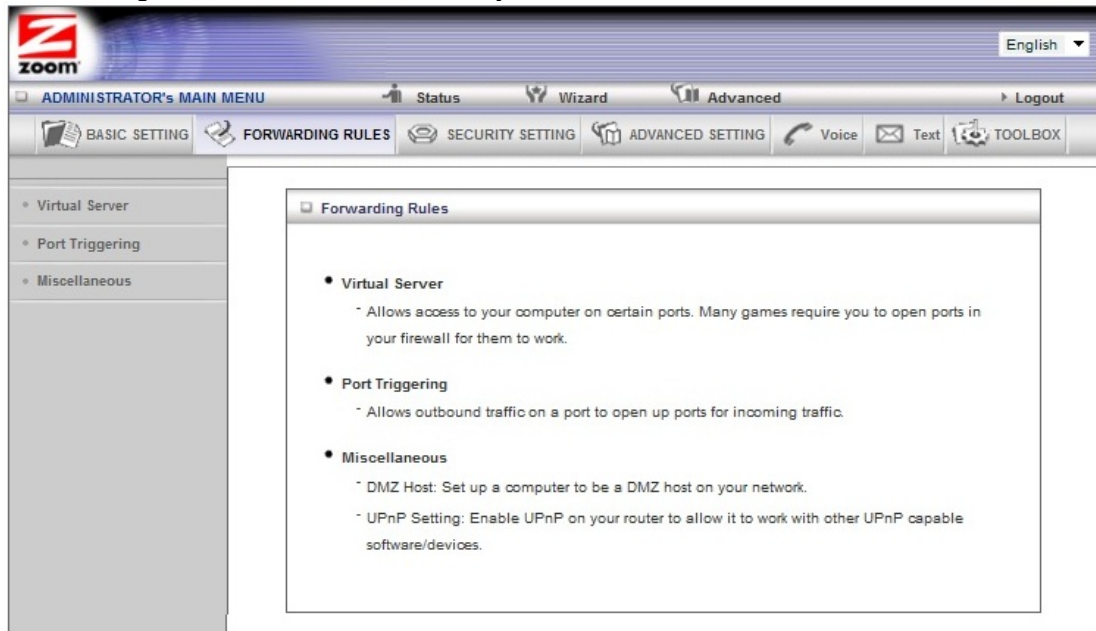
Port triggering works by sensing when data is sent out on the predetermined outgoing port and then automatically opening up the corresponding incoming port(s). It will automatically forward the traffic on the incoming port to the computer that accessed the outgoing port. If your game uses one port to send outgoing data and a different port (or ports) for incoming data, you may want to use port triggering. The advantage of port triggering is that it is more secure than setting up a virtual server since the incoming port is only open when you are using it, and since it tracks which computer

sent the outgoing data. Port triggering can also be easier to set up because you do not need to know the IP address of your gaming station. The disadvantage of port triggering is that only 1 host can be accessing the port at one time, so if you have two computers or game stations playing the same game on your network you will need to use a virtual server or DMZ.

A DMZ differs from a virtual server in that it allows access on all ports of the computer. Because of this, DMZ's are less secure and should be used with caution on your computer. However DMZ's work well with your gaming stations since security is not as much of an issue for gaming stations as it is for computers.

Some games support UPnP. If your game supports UPnP then you do not need to set any forwarding rule since UPnP will automatically set up the Modem/Router to work with the game.

You can use the **Forwarding Rules** page to configure the options mentioned above, for allowing access to devices behind your Modem/Router.



The Virtual Server Page

You can use the **Virtual Server** page to configure a virtual server.

Because your Modem/Router's firewall filters out unrecognized packets to protect your network, all computers behind this product are invisible to the outside world. If you want, you can make some of them accessible by enabling **Virtual Server** mapping.

A virtual server will allow access to your computer on certain ports. A port is like a channel that is used by applications (such as games) to communicate on. For example, the directions for the game you want to play over the Internet might tell you to open port 6000.

Server IP

This is the IP Address of the computer or gaming device that you want to allow access to. If you do not know the IP address you can look it up by selecting **Basic Settings > DHCP Server**, then clicking on **Client List**. To make this virtual server permanent, then you should set up a fixed mapping to your computer or gaming device on the **DHCP Server** page. Doing this ensures that your computer will keep the same IP address

Service Ports

This is the port number you want to allow access to your computer on. To enter multiple ports use the dash format; for example, 2004-2009.

Private Ports

This Modem/Router receives incoming packets on the specified **Service Port(s)**. You can change the destination port to a different port number. The packet is then passed to the LAN using the **Private Port** destination port number..

Protocol

Select **UDP**, **TCP**, or **Both** depending on what type of protocol your game or application uses.

Enable

Click to enable the Virtual Server

Use Rule#

You can enable your virtual server for certain periods of time by assigning it a **Rule #**. You must first set up the appropriate **Scheduling Rule**. See [The Schedule Rule and Schedule Rule Setting Pages](#) on page 82 for more information.

For example, if you have an FTP server (port 21) at 192.168.2.5, a Web server (port 80) at 192.168.2.6, and a game at 192.168.2.7, then you need, at minimum, to specify the following mapping.

ID	Service Port	Server IP	Enable
1	21	192.168.2.5	Yes
2	80	192.168.2.6	Yes
3	5000	192.168.2.7	Yes

The Port Triggering Page

Port triggering opens an incoming port when your computer is using a specified *outgoing port* for specific traffic. This provides a way for you to automate setting up a Virtual Server with some applications. You can use the **Port Triggering** page to configure which packets are allowed access.

The screenshot shows the Zoom! Administrator's Main Menu. The top navigation bar includes 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary bar with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', 'Voice', 'Text', and 'TOOLBOX'. The left sidebar has a tree view with 'Virtual Server', 'Port Triggering' (selected), and 'Miscellaneous'. The main content area is titled 'Port Triggering' and contains a table for configuring port triggering rules. At the top of the table is a dropdown for 'Popular applications' (currently '-- select one --') and a 'Copy to' button. The table has four columns: 'ID', 'Trigger', 'Incoming Ports', and 'Enable'. There are 8 rows, each with an ID from 1 to 8, empty input fields for 'Trigger' and 'Incoming Ports', and a checkbox in the 'Enable' column. At the bottom of the table are 'Save' and 'Undo' buttons.

ID	Trigger	Incoming Ports	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Trigger

The outbound port number used by the application.

Incoming Ports

When the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

Enable

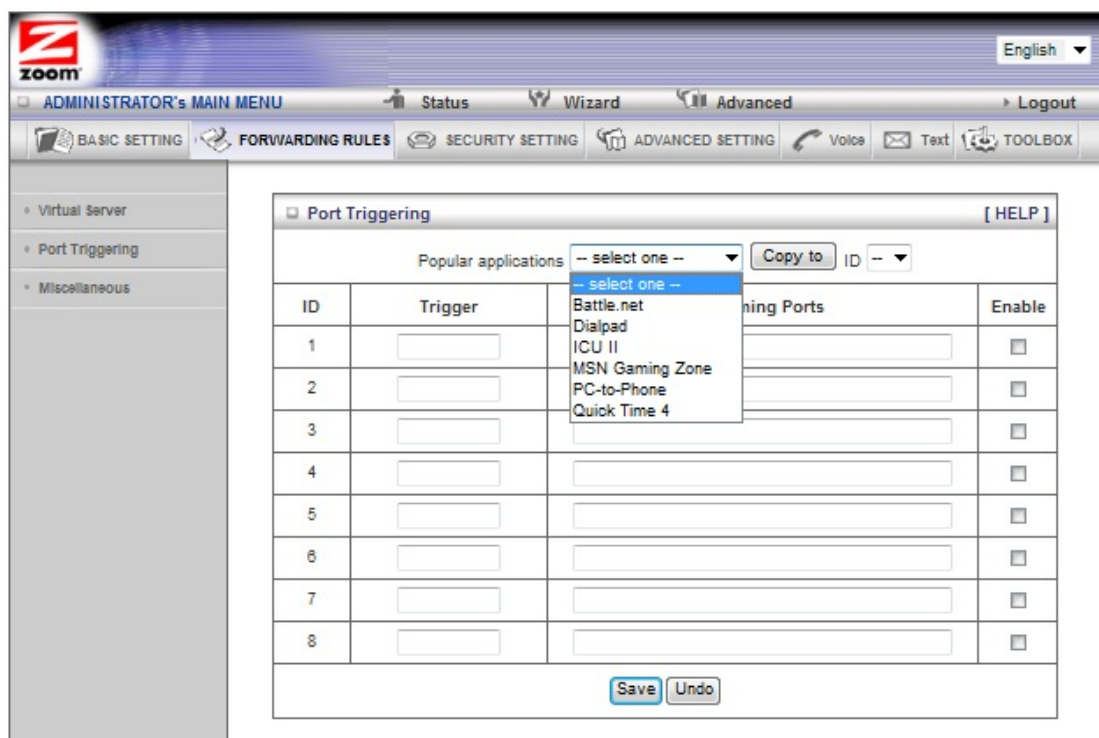
Enables access for the specified application.

Popular applications

Provides a menu of applications from which to choose.

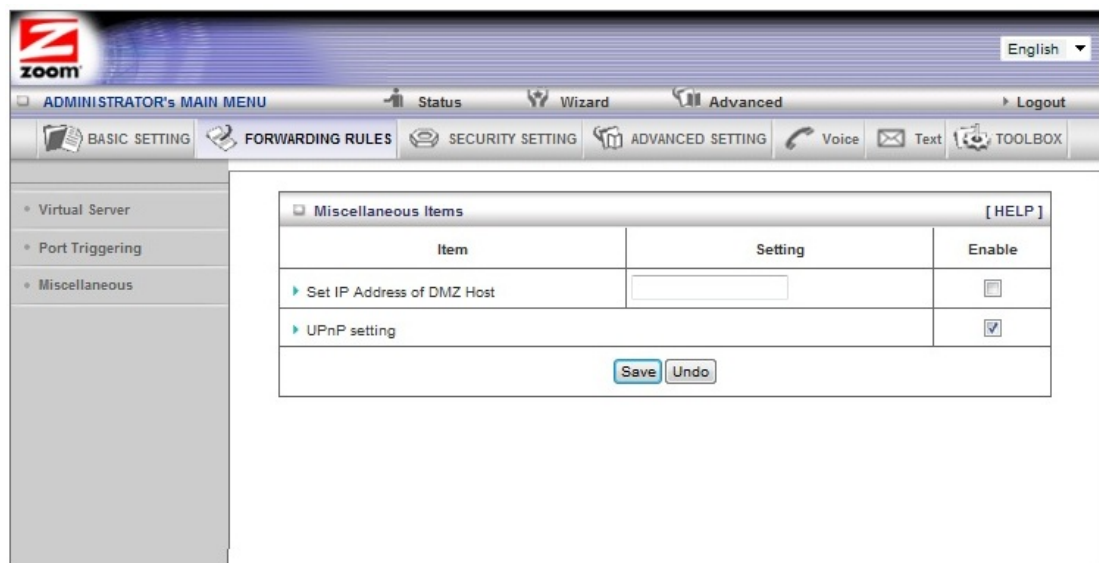
Select an application and click **Copy to** to add the application to your list.

Click **Save** to store your selection or **Undo** to remove the entry.



The Miscellaneous Page

The **Miscellaneous Page** lets you set up and enable a **DMZ Host** on your network, and enable **UPnP** settings for software and devices. In this way, specific ports can open for incoming traffic that must pass through your firewall.



Set IP Address of DMZ Host

A **DMZ** (Demilitarized Zone) **Host** is a host without the protection of the firewall. It allows a computer or gaming system to be exposed to unrestricted two-way communication for Internet games, video conferencing, Internet telephony and other special applications. Use caution when using a

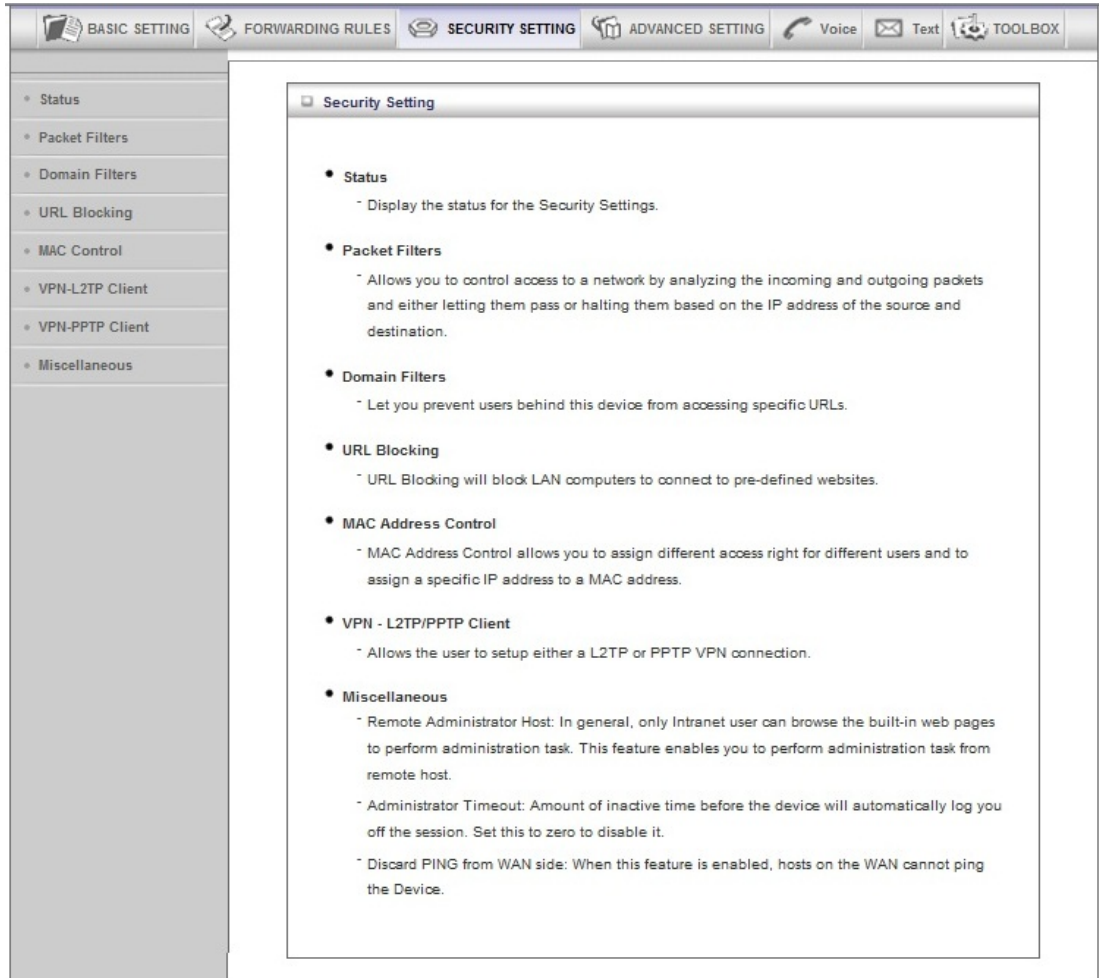
DMZ because your firewall no longer protects the computer that is set up as a DMZ.

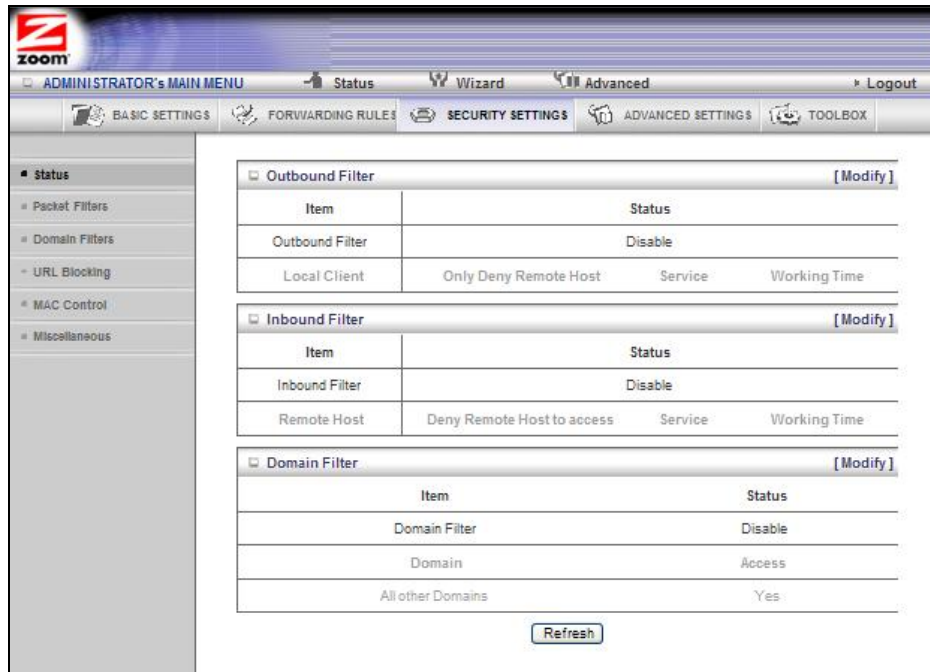
UPnP setting

This feature is enabled by default. Games and applications that are UPnP compatible will automatically open ports for you on your Modem/Router.

Configuring Security Settings

The **Security Setting** page lists eight configuration menus on the left pane and provides a description of the configuration menus at center.





Status Page

The **Status** page shows you the status of the inbound and outbound **Packet Filters** and the Domain Filters. **Inbound**, **Outbound**, and **Domain** filters are disabled, by default.

Packet Filtering Page

Packet Filtering allows you to control what packets are allowed to pass through the Modem/Router. Outbound Packet filters control outbound packets and Inbound Filtering controls packets coming from the Internet. Inbound Filters applies only to packets going to a Virtual Server or DMZ. Most users will not need to setup Packet Filtering.

When you click on **Packet Filters** from the left-side menu, it takes you to the **Outbound Packet Filtering page**. If you need to set up an Inbound Filter, click on **Inbound Filter** button at the bottom of the page.

Filtering Policies

You can select one of the two filtering policies:

Allow all to pass except those that match the specified rules

Deny all to pass except those that match the specified rules

Filtering Rules

You can specify eight rules for each direction: inbound or outbound. For each rule, you can define the following:

Source IP address

Destination IP address**Destination Port****Use Rule#**

For the **Source** or **Destination IP address**, you can define a single IP address (4.3.2.1). An empty field implies any IP address.

For **Destination Port**, you can define a single port (80) or a range of ports (1000-1999). No prefix indicates both TCP and UDP are defined. Leaving this empty implies that all port addresses apply.

Each **Rule** can be enabled or disabled individually.

You can use packet filters with scheduling rules for more access control flexibility.

The Domain Filters Page

You can use the **Domain Filters** page to enable or deny user access to specified URLs. Domain filtering and URL Blocking perform similar functions. The major difference between Domain Filtering and URL Blocking is that Domain Filtering requires the user to input a suffix whereas URL Blocking requires the user to input a keyword only. In other words, Domain Filtering can block a specific web site, whereas URL Blocking can block hundreds of web sites by specifying a keyword.

Domain Filter

Use to prevent users behind this device from accessing specific URLs.

Log attempted URL Access

Check if you want to log the action when someone accesses the specific URLs.

Privilege IP Address Range

Domain filtering rules do not apply to IP addresses in this range.

Domain Suffix

The suffix of the restricted URL; for example, **xxx.com**.

Action

The action to be taken when a user accesses the restricted domain suffix URL. Check **Drop** to block access. Check **log** to record the attempted access.

Enable

Click the checkbox to enable a rule.

The URL Blocking Page

You can use the **URL Blocking** page to block LAN computers from connecting to pre-defined Web sites or to limit their access to specific websites. The major difference between Domain Filtering and URL Blocking is that Domain Filtering requires the user to input a suffix whereas URL Blocking requires the user to input a keyword only. In other words, Domain Filtering can block a specific web site, whereas URL Blocking can block hundreds of web sites by specifying a keyword.

URL Blocking [HELP]			
Item		Setting	
▶ URL Blocking		<input type="checkbox"/> Enable	
▶ Block Setting		<input checked="" type="radio"/> Blacklist <input type="radio"/> Whitelist	
ID	URL	Enable	Use Rule#
1	<input type="text"/>	<input type="checkbox"/>	(0) Always ▼
2	<input type="text"/>	<input type="checkbox"/>	(0) Always ▼
3	<input type="text"/>	<input type="checkbox"/>	(0) Always ▼
4	<input type="text"/>	<input type="checkbox"/>	(0) Always ▼
5	<input type="text"/>	<input type="checkbox"/>	(0) Always ▼
6	<input type="text"/>	<input type="checkbox"/>	(0) Always ▼
7	<input type="text"/>	<input type="checkbox"/>	(0) Always ▼
8	<input type="text"/>	<input type="checkbox"/>	(0) Always ▼
9	<input type="text"/>	<input type="checkbox"/>	(0) Always ▼
10	<input type="text"/>	<input type="checkbox"/>	(0) Always ▼

Save Undo

URL Blocking Enable

Check if you want to enable URL Blocking.

Block Setting

Select Blacklist to block access to any words or URLs that you specify.
Select Whitelist to allow access only to the URLs that you specify.

URL

If any part of the Website's URL matches the pre-defined word, the connection will be blocked if Blacklist is set, or allowed if Whitelist is set. For example, if you set up blacklisting, you can use the pre-defined word, sex, to block all website URLs that contain the pre-defined word, sex.

Enable

Click the checkbox to enable each rule.

The MAC Control Page

You can use the **MAC Control** page to provide an added layer of security to your Modem/Router. MAC Address control is used to define connection and association rights for clients whose IP and MAC addresses are specified. Click on the **HELP** button page for a detailed explanation including examples for setting up MAC address control.

MAC Address Control [HELP]

Item	Setting
MAC Address Control	<input type="checkbox"/> Enable
Connection control	<input type="checkbox"/> Wireless and wired clients with C checked can connect to this device; and unspecified MAC addresses to connect. allow
Association control	<input type="checkbox"/> Wireless clients with A checked can associate to the wireless LAN; and unspecified MAC addresses to associate. allow

DHCP clients -- select one -- Copy to ID --

ID	MAC Address	IP Address	C	A	Use Rule#
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	(0) Always
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	(0) Always
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	(0) Always
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	(0) Always
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	(0) Always

<< Previous Next >> Save Undo

MAC Address Control

Check **Enable** to enable **MAC Address Control**. All of the settings on this page will take effect only if **Enable** is checked.

Connection control

Check **Connection control** to specify which wired and wireless clients can connect to this device. If a client is denied a connection to this device, then that client is also denied Internet access. Choose **allow** or **deny** to indicate which clients can connect to this device.

Association control

Check **Association control** to specify which wireless clients can associate to the wireless LAN. If a client is not allowed to associate to the wireless LAN, then the client can't send or receive any data via this device. Choose **allow** or **deny** to indicate which clients can associate to the wireless LAN. If selected, the specified wireless client will obtain any radio connection to the access point.

DHCP clients

Displays a list of computers that are currently connected to the Modem/Router. Select a client from the menu then copy to the selected ID. The client IP and MAC addresses are written in the fields below the menus.

The VPN-L2TP Client Page

You can use the **VPN-L2TP Client** page to set up a L2TP client to securely access your corporate network.

VPN-L2TP Client

Check **Enable** to enable the L2TP client on the Modem/Router. To set up the client, click on **Edit** and enter the parameters for your network. To enable a L2TP client click the **Enable** box next to the client you created. To disable the client uncheck the **Enable** box.

The VPN-PPTP Client Page

You can use the **VPN-PPTP Client** page to set up a PPTP client to securely access your corporate network.

Check **Enable** to enable the PPTP client on the Modem/Router. To set up the client, click on **Edit** and enter the parameters for your network. To enable a PPTP client click the **Enable** box next to the client you created. To disable the client uncheck the **Enable** box

The Miscellaneous Page

You can use the **Miscellaneous Items** page to enable additional security features.

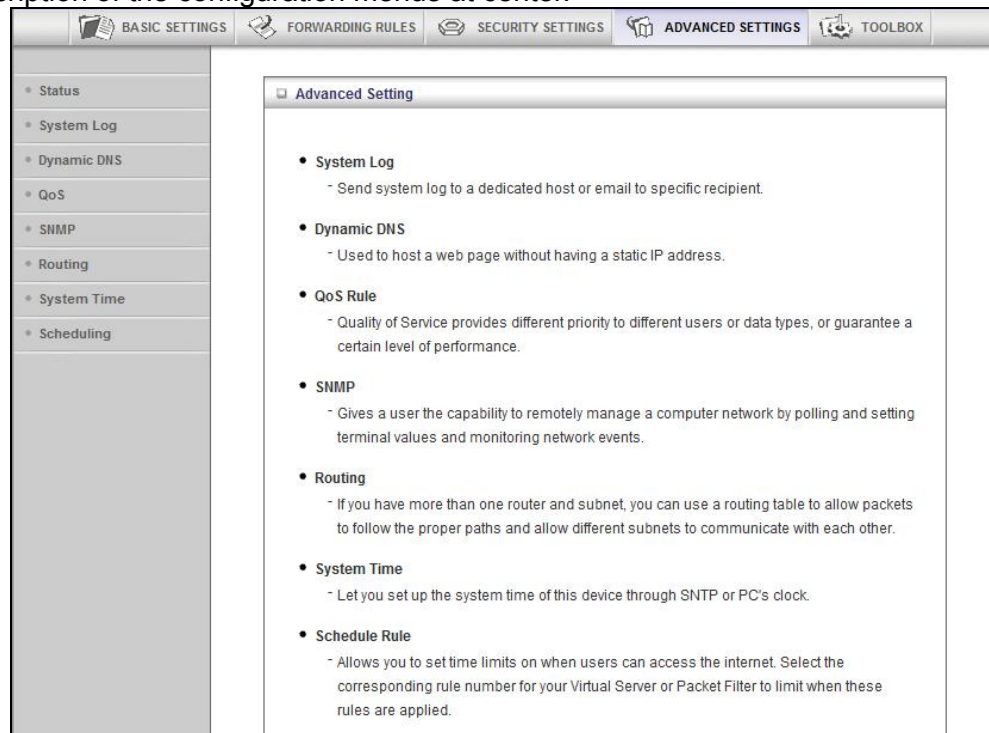
Miscellaneous Items [HELP]		
Item	Setting	Enable
▶ Administrator Time-out	0 seconds (0 to disable)	
▶ Remote Administrator Host : Port	/ :	<input type="checkbox"/>
▶ Discard PING from WAN side		<input type="checkbox"/>
▶ DoS Attack Detection		<input type="checkbox"/>
▶ Non-Standard FTP Port		
▶ Disable PPTP Passthrough		<input type="checkbox"/>
▶ Disable L2TP Passthrough		<input type="checkbox"/>
▶ Disable IPSec Passthrough		<input type="checkbox"/>
▶ NAT Loopback		<input type="checkbox"/>
▶ IGMP Proxy		<input type="checkbox"/>
▶ Stealth Mode		<input checked="" type="checkbox"/>

Save Undo

Please refer to the online help for details about each of the menu items.

Configuring Advanced Settings

The **Advanced Settings** page lists eight menus on the left pane and provides a description of the configuration menus at center.



The System Log Page

You can use the **System Log** page to define how and where system logs will be exported via syslog (UDP) or SMTP(TCP).

The screenshot shows the 'System Log' configuration page. It includes a sidebar with the same eight menu items as the previous page, with 'System Log' selected. The main area contains a table for configuration:

Item	Setting	Enable
IP address for syslogging	<input type="text"/>	<input type="checkbox"/>
Email alert settings		<input type="checkbox"/>
SMTP Server : port	<input type="text"/> : <input type="text"/>	
SMTP Username	<input type="text"/>	
SMTP Password	<input type="text"/>	
E-mail addresses	<input type="text"/>	
E-mail subject	<input type="text"/>	

At the bottom, there are buttons for 'Save', 'Undo', 'View Log...', and 'Email Log Now'.

IP Address for Syslogging

Host IP address of the destination where the Sys log will be sent.
Click the **Enable** checkbox to set the IP Address as the destination.

E-mail alert settings

Check **Enable** if you want to send **syslog** via email.

SMTP Server IP and Port

Input the SMTP server IP and port; for example, **mail.your_url.com** or **192.168.2.100:26**. If you do not specify a port number, the port value will be set to 25.

SMTP Username and Password

Input the SMTP Username and Password.

E-mail addresses

The email address of each **syslog** recipient.

E-mail Subject

The subject of the email alert. This setting is optional.

The Dynamic DNS Page

You can use the **Dynamic DNS** page to define the **Dynamic Domain Name Service (DDNS)** that will host your server. For example, the **DDNS** could host your server when you want to host a website on your network but you do not have a static IP. Your DDNS provider keeps track of changes to your IP address and automatically routes users trying to access your web site to the correct location

Note: Before you enable **DDNS**, you must register an account with one of the **DDNS** servers listed in the **Provider** field.

The screenshot shows a web interface with a top navigation bar containing tabs: BASIC SETTINGS, FORWARDING RULES, SECURITY SETTINGS, ADVANCED SETTINGS, and TOOLBOX. The left sidebar has a menu with items: Status, System Log, Dynamic DNS (selected), QoS, SHMP, Routing, System Time, and Scheduling. The main content area is titled 'Dynamic DNS' with a '[HELP]' link. It contains a table with two columns: 'Item' and 'Setting'. The table has five rows: 1. 'DDNS' with a radio button set to 'Disable' (with 'Enable' also visible). 2. 'Provider' with a dropdown menu showing 'DynDNS.org(Dynamic)'. 3. 'Host Name' with an empty text input field. 4. 'Username / E-mail' with an empty text input field. 5. 'Password / Key' with an empty text input field. Below the table are 'Save' and 'Undo' buttons.

Item	Setting
DDNS	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Provider	DynDNS.org(Dynamic)
Host Name	<input type="text"/>
Username / E-mail	<input type="text"/>
Password / Key	<input type="text"/>

Save Undo

Your DDNS provider will provide the **HostName**, **Username/E-mail**, and **Password/Key** that you will enter into the fields on the **Dynamic DNS** page.

The QoS Page

You can use the **Quality of Service (QoS)** page to provide different priorities to different users or data flows, or to guarantee a certain level of performance.

QoS Rule [HELP]					
Item		Setting			
QoS Control		<input type="checkbox"/> Enable			
Available Upstream bandwidth		<input type="text"/> kbps (Kilobits per second)			
ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use Rule#
1	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	(0) Always
2	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	(0) Always
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	(0) Always
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	(0) Always
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	(0) Always
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	(0) Always
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	(0) Always
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	(0) Always

Save Undo

QoS Control

Click the **Enable** checkbox to enable QoS.

Available Upstream bandwidth

Set the upstream speed. The best way to find your throughput is to use one of the free speed tests widely available on the Web. Some examples of sites with good speed tests are www.speedtest.net and www.speakeasy.net/speedtest. When you know your actual upstream throughput, enter it in this field. The value should be in kilobits per second (Kbps).

Local: IP

Define the local IP address of packets.

Local: Ports

Define the local port of packets.

Remote: IP

Define the remote IP address of packets.

Remote: Ports

Define the remote port of packets.

QoS Priority

Select a value from the dropdown menu to define the priority level for the local and remote settings. Packets will be serviced based upon the priority level set. For critical applications, select **High** or **Normal**. For non-critical

applications, select **Low**. **High** is the default value.

Enable

Click the **Enable** checkbox to apply the settings.

User Rule#

Select a rule from the dropdown menu to indicate when the policy applies. **(0)** **Always** is the default value.

The SNMP Page

You can use the **Simple Network Management Protocol (SNMP)** page to set up the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events. Most users do not need to set up SNMP.

Item	Setting
Enable SNMP	<input type="checkbox"/> Local <input type="checkbox"/> Remote
Get Community	<input type="text"/>
Set Community	<input type="text"/>
IP 1	<input type="text"/>
IP 2	<input type="text"/>
IP 3	<input type="text"/>
IP 4	<input type="text"/>
SNMP Version	<input checked="" type="radio"/> V1 <input type="radio"/> V2c
WAN Access IP Address	<input type="text"/>

Save Undo

Enable SNMP

Click the **Local**, **Remote**, or both checkboxes to enable the SNMP function. Check **Local** if you want the Modem/Router to respond to requests from the LAN. Check **Remote** if you want the Modem/Router to respond to requests from the WAN.

Get Community

Set **Get Community** to the **GetRequest** to which your device will respond.

Set Community

Set **Set Community** to the **SetRequest** that your device will accept.

IP 1, IP 2, IP 3, IP 4

Enter the IP address of your SNMP Management PCs. You must specify where the Modem/Router should send **SNMP Trap** messages.

SNMP Version

Select the **SNMP Version** that your SNMP Management software supports.

WAN Access IP Address

Enter the IP address for WAN access. The default value of **0.0.0.0** indicates that every IP address can get some information about this device, using the SNMP protocol.

The Routing Table Page

You can use the **Routing Table** page to enable/disable both **Dynamic** and **Static Routing**. If routing is enabled, you can specify which physical interface address to use for outgoing IP data grams. If you have more than one Modem/Router and subnet, you will need to define a routing table that lets packets find the proper routing path and allows different subnets to communicate with each other. Most users do not need to set up Dynamic or Static Routing.

Routing Table [HELP]					
Item		Setting			
▶ Dynamic Routing		<input checked="" type="radio"/> Disable <input type="radio"/> RIPv1 <input type="radio"/> RIPv2			
▶ Static Routing		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Dynamic Routing

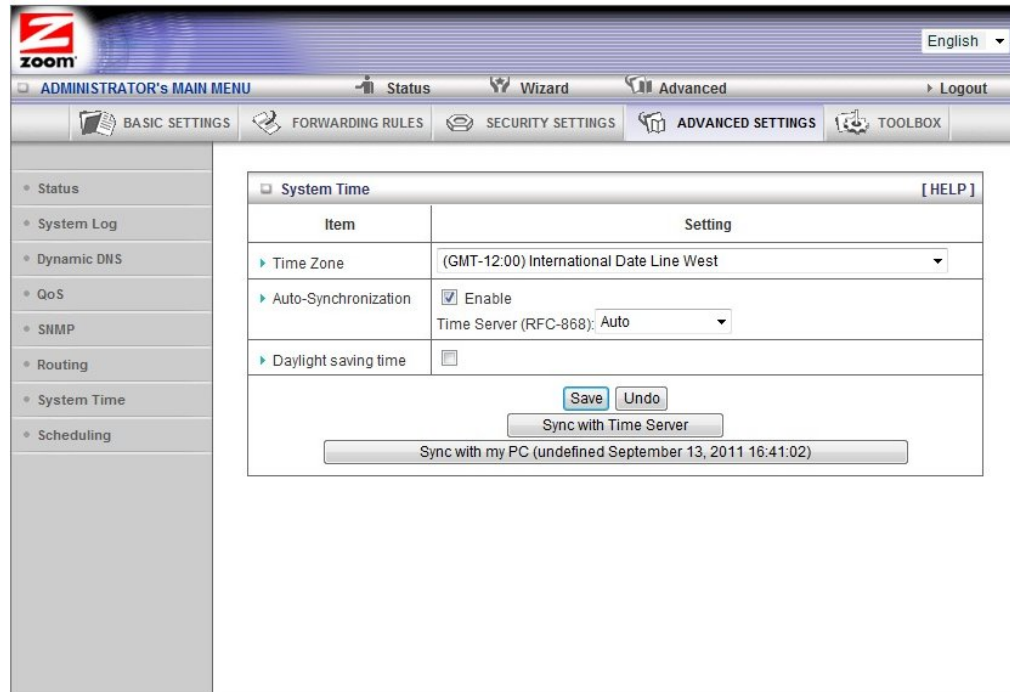
The **Routing Information Protocol (RIP)** will exchange information about destinations for computing routes throughout the network. Please select **RIPv2** only if you have different subnet in your network. Otherwise, please select **RIPv1** if you need this protocol.

Static Routing

For static routing, you can specify up to eight routing rules. You can enter the **Destination** IP address, **Subnet Mask**, **Gateway**, **Hop** for each routing rule. Click the **Enable** checkbox to activate the routing table entry.

The System Time Page

You can use the **System Time** page to set and synchronize your Modem/Router with the local time zone, the Time Server and your PC.



The screenshot shows the 'System Time' configuration page in the Zoom! web interface. The page has a sidebar with a menu containing: Status, System Log, Dynamic DNS, QoS, SNMP, Routing, System Time (selected), and Scheduling. The main content area is titled 'System Time' and contains a table with the following items and settings:

Item	Setting
Time Zone	(GMT-12:00) International Date Line West
Auto-Synchronization	<input checked="" type="checkbox"/> Enable Time Server (RFC-868): Auto
Daylight saving time	<input type="checkbox"/>

Below the table, there are buttons for 'Save', 'Undo', and 'Sync with Time Server'. At the bottom, there is a button for 'Sync with my PC (undefined September 13, 2011 16:41:02)'.

Time Zone

Select the local time zone from the dropdown menu.

Auto-Synchronization

Click the **Enable** checkbox to enable this function.

Select an item from the **Time Server** dropdown menu to specify the server with which to synchronize. The default value is **Auto**.

Click **Sync with Time Server** to set **Date** and **Time** by NTP Protocol.

Click **Sync with my PC** to set **Date** and **Time** using your PC's Date and Time

Daylight Saving time

Select enable if you live in an area that uses daylight savings time. You need to enter the start and end dates for daylight savings time.

The Schedule Rule and Schedule Rule Setting Pages

You can use the **Schedule Rule** and **Schedule Rule Setting** pages to define when services will be turned on and off based on rules that you define.

- 1 On the **Schedule Rule** page, click the **Enable** checkbox to enable the scheduling rules, which are defined on the **Schedule Rule Setting** page.

The screenshot shows the 'Schedule Rule' page. On the left is a sidebar menu with options: Status, System Log, Dynamic DNS, QoS, SHMP, Routing, System Time, and Scheduling. The main content area has a top navigation bar with 'BASIC SETTINGS', 'FORWARDING RULES', 'SECURITY SETTINGS', 'ADVANCED SETTINGS', and 'TOOLBOX'. Below this, the 'Schedule Rule' section is active, showing a table with columns 'Rule#' and 'Rule Name'. There are 10 rows, each with a 'New Add' button. At the bottom, there are buttons for '<< Previous', 'Next >>', 'Save', and 'Add New Rule...'. A checkbox labeled 'Enable' is also present.

Rule#	Rule Name	Action
1		New Add
2		New Add
3		New Add
4		New Add
5		New Add
6		New Add
7		New Add
8		New Add
9		New Add
10		New Add

- a. Click **Add New Rule** to open the **Schedule Rule Setting** page.

The screenshot shows the 'Schedule Rule Setting' page. It has the same sidebar and top navigation bar as the previous page. The 'Schedule Rule Setting' section is active, showing a form for configuring a rule. It includes fields for 'Name of Rule 1', 'Policy' (set to 'Inactivate'), and a table for 'Week Day' with columns for 'ID', 'Week Day', 'Start Time (hh:mm)', and 'End Time (hh:mm)'. There are 8 rows for the week days. At the bottom, there are buttons for 'Save', 'Undo', and 'Back'.

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose day --		
2	-- choose day --		
3	-- choose day --		
4	-- choose day --		
5	-- choose day --		
6	-- choose day --		
7	-- choose day --		
8	-- choose day --		

- b. On the **Schedule Rule Setting** page, specify a **Rule name**, a **Policy** that defines whether the rule is **Active** or **Inactive**, **Week Day** and the **Start Time** and **End Time** for each rule that you are creating.

[BASIC SETTINGS](#)
[FORWARDING RULES](#)
[SECURITY SETTINGS](#)
[ADVANCED SETTINGS](#)
[TOOLBOX](#)

- Status
- System Log
- Dynamic DNS
- QoS
- SNMP
- Routing
- System Time
- Scheduling

Schedule Rule Setting
[HELP]

Item		Setting	
Name of Rule 1		test1	
Policy		Inactivate except the selected days and hours below.	
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	Monday	09:00	10:00
2	-- choose day --		
3	-- choose day --		
4	-- choose day --		
5	-- choose day --		
6	-- choose day --		
7	-- choose day --		
8	-- choose day --		

Save
Undo
Back

- Click **Save** for each rule that you create.
- Click **Back** to return to the **Schedule Rule** page.
- When the **Schedule Rule** page opens, the rule(s) that you created and saved appear in the **Rule Name** column.

[BASIC SETTINGS](#)
[FORWARDING RULES](#)
[SECURITY SETTINGS](#)
[ADVANCED SETTINGS](#)
[TOOLBOX](#)

- Status
- System Log
- Dynamic DNS
- QoS
- SNMP
- Routing
- System Time
- Scheduling

Schedule Rule
[HELP]

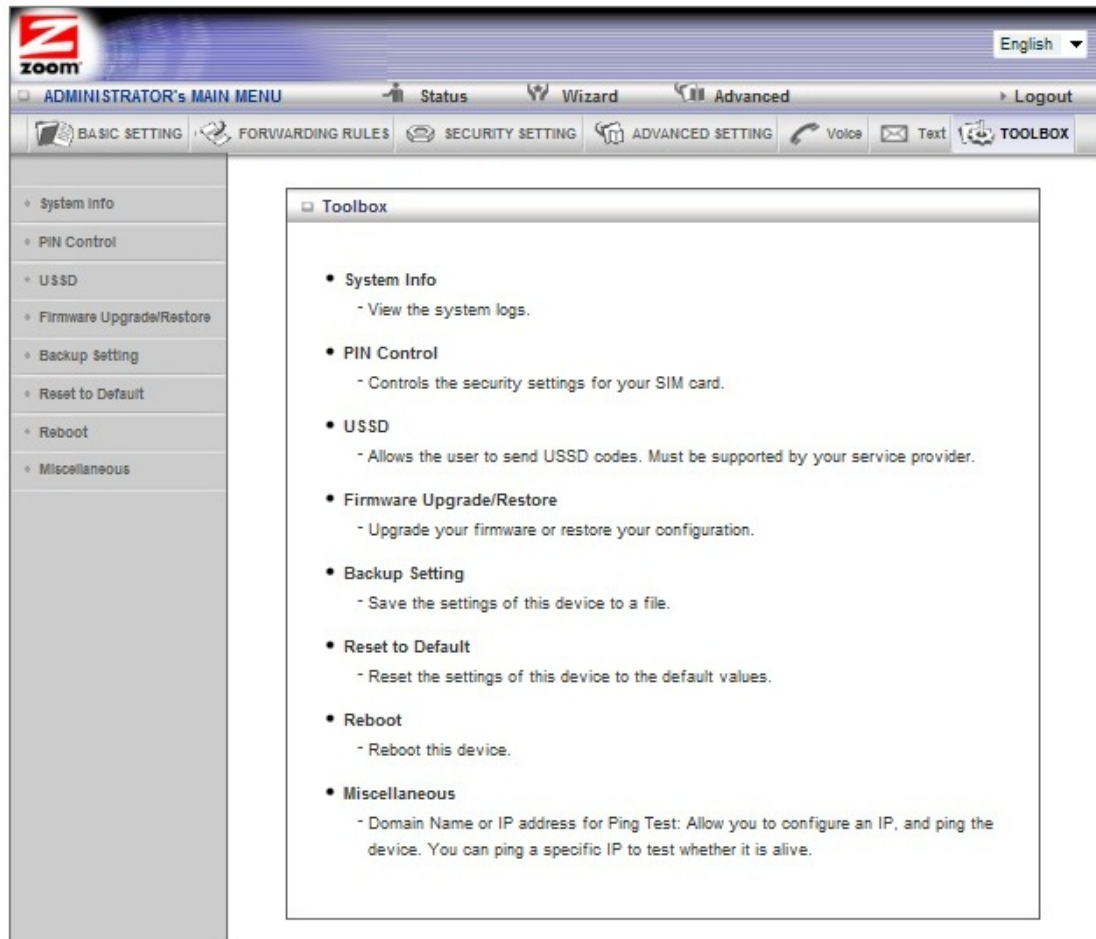
Item		Setting	
Schedule		<input checked="" type="checkbox"/> Enable	
Rule#	Rule Name	Action	
1	test1	Edit Delete	
2	test2	Edit Delete	
3	test3	Edit Delete	
4		New Add	
5		New Add	
6		New Add	
7		New Add	
8		New Add	
9		New Add	
10		New Add	

<< Previous
Next >>
Save
Add New Rule...

- Click **Edit** to make changes to a scheduled rule.
- Click **Delete** to remove a scheduled rule.

Configuring Toolbox Settings

The **Toolbox Settings** page lists eight configuration menus on the left pane and provides a description of the configuration menus at center.

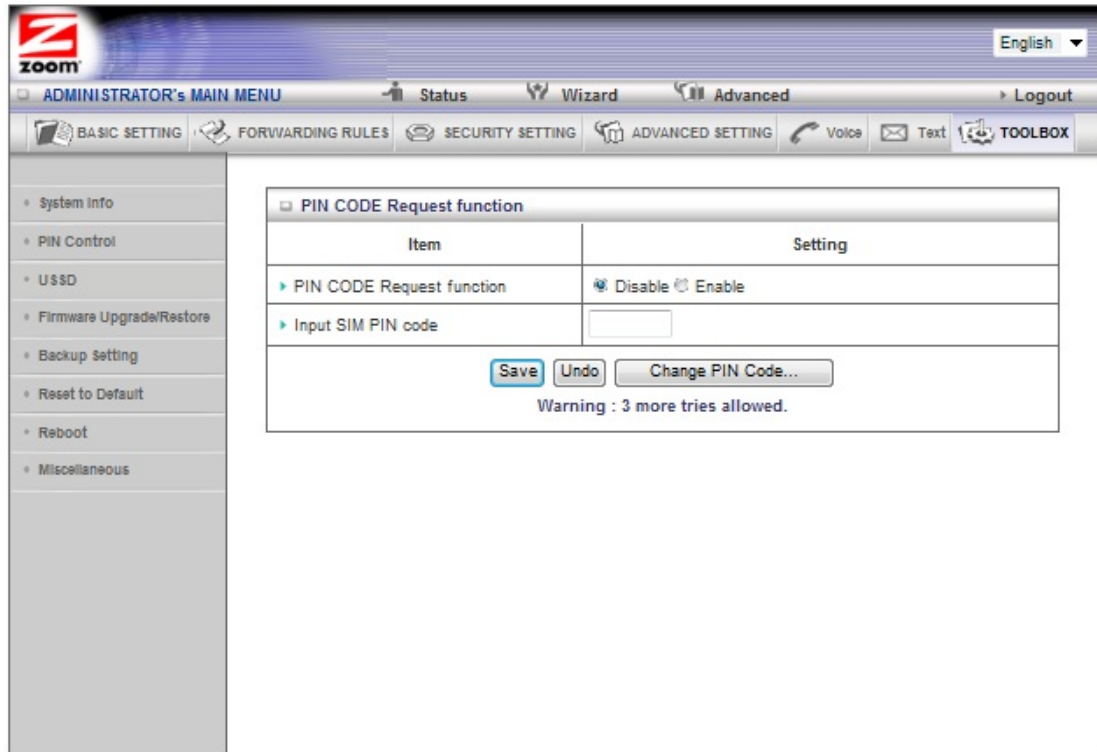


The System Information Page

You can use the **System Information** page to view information about your Modem/Router, and to view download, and delete system logs.

The Pin Control Page

Your service provider may provide you with a pin code to protect your SIM card from unauthorized use or you may want to request a pin code from your service provider if you are concerned about your SIM card being removed from your Modem/Router and used with another device without your permission.



The screenshot shows the Zoom Modem/Router Administrator's Main Menu. The left sidebar contains a list of menu items: System Info, PIN Control, USSD, Firmware Upgrade/Restore, Backup Setting, Reset to Default, Reboot, and Miscellaneous. The main content area displays the 'PIN CODE Request function' settings. It includes a table with two columns: 'Item' and 'Setting'. The first row shows 'PIN CODE Request function' with radio buttons for 'Disable' (selected) and 'Enable'. The second row shows 'Input SIM PIN code' with a text input field. Below the table are buttons for 'Save', 'Undo', and 'Change PIN Code...'. A warning message states: 'Warning : 3 more tries allowed.'

Item	Setting
PIN CODE Request function	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Input SIM PIN code	<input type="text"/>

Warning : 3 more tries allowed.

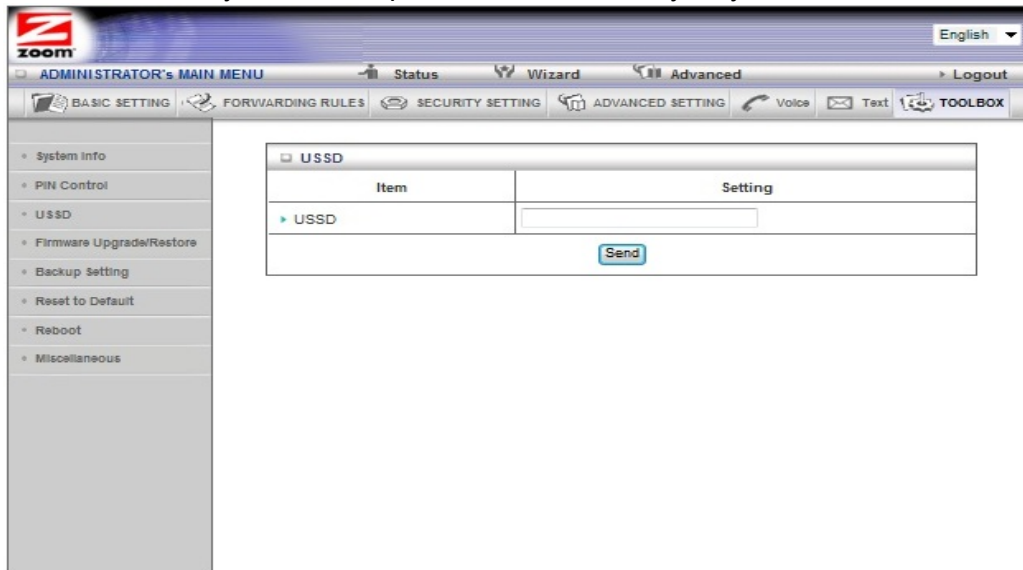
To use a pin code with your Modem/Router click **Enable** next to the **PIN CODE Request function** and enter the 4 digit pin code given to you by your service provider. For security reasons, you are only allowed 3 attempts to enter your pin code correctly. If you fail to enter your pin code correctly after 3 attempts, you will be asked to enter a PUK code. If you are prompted for a PUK code you must call your service provider and request the PUK code from them. This is done to prevent unauthorized users from guessing your PIN code.

If you want to change the 4 digit pin code given to you by your service provider click the **Change PIN Code** button.

Note: After you enable the pin code, you do not need to enter it each time you use the Modem/Router. You would only need to enter the pin code if you reset the modem using the reset button on the front panel or if you restored the modem to factory defaults by using the **Reset to Default** command on page 87.

The USSD Page

Your Modem/Router supports USSD codes. These are typically used to request information from your service provider in a fast, easy way.



The screenshot shows the Zoom Administrator's Main Menu. The left sidebar contains a list of menu items: System Info, PIN Control, USSD, Firmware Upgrade/Restore, Backup Setting, Reset to Default, Reboot, and Miscellaneous. The main content area is titled 'ADMINISTRATOR'S MAIN MENU' and includes tabs for Status, Wizard, and Advanced. Below these tabs are icons for BASIC SETTING, FORWARDING RULES, SECURITY SETTING, and ADVANCED SETTING. The 'ADVANCED SETTING' tab is selected, and the 'USSD' sub-tab is active. The USSD configuration page displays a table with two columns: 'Item' and 'Setting'. The 'Item' column contains a dropdown menu with 'USSD' selected. The 'Setting' column contains a text input field. A 'Send' button is located below the input field.

Item	Setting
USSD	<input type="text"/>

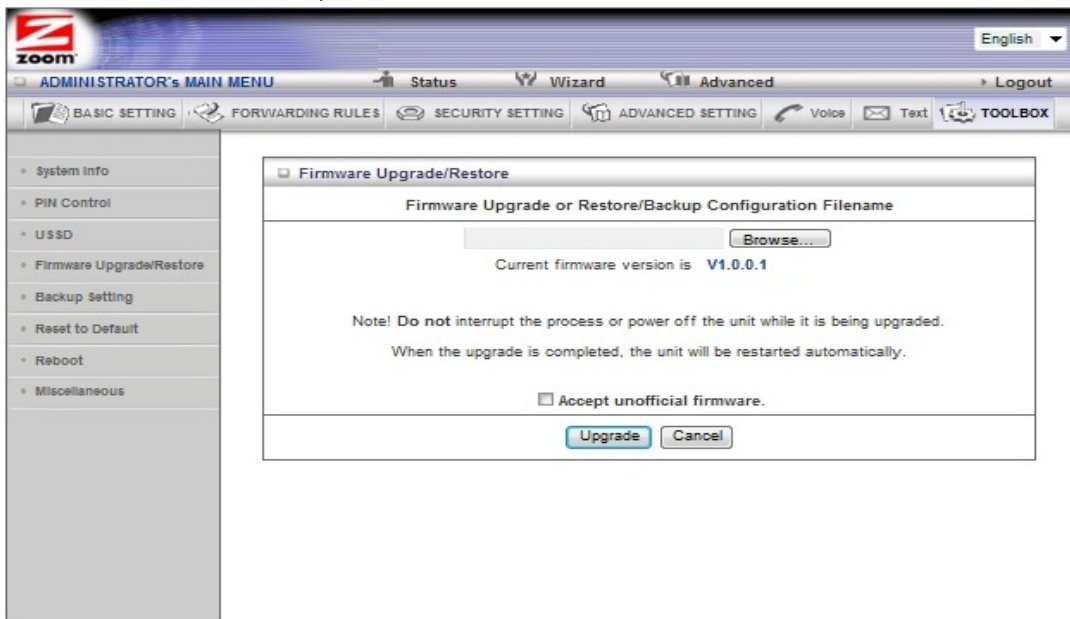
Enter a USSD number in the **Setting** field and click **Send** to send it to your service provider to get information from that service provider.

If you want to check if your service provider supports USSD codes, we suggest that you search this phrase using Google or some other search engine:

<your service provider name> USSD

The Firmware Upgrade Page

You can use the **Firmware Upgrade** page to get the most recent version of the Modem/Router firmware, if available.



The screenshot shows the Zoom Administrator's Main Menu with the 'Firmware Upgrade/Restore' page selected. The left sidebar is the same as in the previous screenshot. The main content area shows the 'Firmware Upgrade/Restore' sub-tab. The page title is 'Firmware Upgrade/Restore'. Below the title is a section titled 'Firmware Upgrade or Restore/Backup Configuration Filename'. This section contains a text input field with a 'Browse...' button next to it. Below the input field, it states 'Current firmware version is V1.0.0.1'. A note follows: 'Note! Do not interrupt the process or power off the unit while it is being upgraded. When the upgrade is completed, the unit will be restarted automatically.' Below the note is a checkbox labeled 'Accept unofficial firmware.' At the bottom of the section are 'Upgrade' and 'Cancel' buttons.

Firmware Upgrade/Restore

Firmware Upgrade or Restore/Backup Configuration Filename

Current firmware version is V1.0.0.1

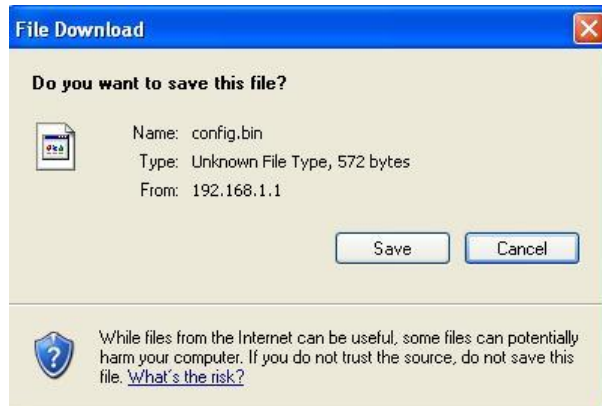
Note! Do not interrupt the process or power off the unit while it is being upgraded.
When the upgrade is completed, the unit will be restarted automatically.

☐ Accept unofficial firmware.

- 1 Click **Browse** to open the location where you saved the **Firmware Update** file that you downloaded from the Zoom web site or received via email. If you are restoring a saved configuration file, select the file that your configuration is saved in.
- 2 Click **Upgrade**.

The Backup Setting Dialog

You can back up your Modem/Router settings by clicking the **Backup Setting** item from the left pane of the Toolbox menu. The following dialog opens.



- 1 Click **Save** to write and save your Modem/Router settings as a binary file.

The Reset to Default Dialog

You can reset the Modem/Router to its factory settings by clicking the **Reset to Default** item from the left pane of the Toolbox menu. The following dialog opens.



- 1 Click **OK** to reset the Modem/Router.
We recommend that you back up and save your configuration first if you've made changes and want a record of that configuration

The Reboot Dialog

You can reboot the Modem/Router by clicking the **Reboot** item from the left pane of the Toolbox menu. The following dialog opens.



- 1 Click **OK** to reboot the Modem/Router.

The Miscellaneous Page

You can use this page to **Ping** a remote device on your network or to wake up a PC on your network that is in sleep mode. The remote PC must be configured for **Wake-on-LAN** mode

The screenshot shows the 'ADMINISTRATOR'S MAIN MENU' for a Zoom modem/router. The left sidebar lists various system settings, with 'Miscellaneous' selected. The main content area is titled 'Miscellaneous Items' and contains a table for configuring wake-on-LAN and ping test settings.

Item	Setting
▶ MAC Address for Wake-on-LAN	<input type="text"/> <input type="button" value="Wake up"/>
▶ Domain Name or IP address for Ping Test	<input type="text"/> <input type="button" value="Ping"/>

At the bottom of the table are and buttons.

Appendix A: Mobile Broadband Settings

This chart lists **APN**, **Dialed Number**, **Username**, and **Password** settings for different providers. If auto-configure did not work you may need to manually enter the settings for your provider. For instructions on how to do this, please refer to [Chapter 7: Using the Configuration Manager's Advanced Program](#).

If you are unable to connect to the Internet using the Modem/Router, you should try entering the different settings for your service provider. Begin by entering the first setting for your provider. If that doesn't work, try entering the next setting. If a field is empty in the chart, then leave that setting blank.

U.S. Mobile Broadband Service Providers

Provider	APN	Dialed Number for 3G	Dialed Number for 4G	Username	Password	Other Settings
AT&T (1)	Check with provider	*99#	*99***3# OR *99***1#			
AT&T (2)	ISP.CINGULAR	*99***1#	*99***3# OR *99***1#			
AT&T (3)	ISP.CINGULAR	*99#	*99***3# OR *99***1#	WIXDC001@W5.MYCINGULAR.COM	CINGULAR1	
AT&T voice/data or iPhone SIM card	WAP.CINGULAR	*99#	*99***3# OR *99***1#	WAP@CINGULAR.COM	CINGULAR1	
Cingular ex-AT&T	proxy			guest	guest	
Cingular with acceleration	ISP.CINGULAR			ISPDA@CINGULARGPRS.COM	CINGULAR1	
Cingular w/o acceleration	ISP.CINGULAR			ISP@CINGULARGPRS.COM	CINGULAR1	
Cingular non-contract	WAP.CINGULAR			WAP@CINGULARGPRS.COM	CINGULAR1	
T-Mobile	Check with provider	*99#	*99***3# OR *99***1#			
T-Mobile US GPRS Internet	internet2.voicestream.com					

T-Mobile Internet	internet2.voicestream.com			guest	guest	
T-Mobile VPN	internet3.voicestream.com			guest	guest	
T-Mobile non-contract	wap.voicestream.com			guest	guest	

U.K. Mobile Broadband Service Providers

Provider	APN	Dialed Number	Username	Password	Other Settings
3	three.co.uk		guest	guest	
Anvil Mobile (1)	m2m.sim4life.com	*99#			
Anvil Mobile (2)	m2m.aql.net	*99#			
ASDA	asdamobiles.co.uk		wap	wap	Gateway Address: 212.183.137.12
BT Mobile Business	btmobile.bt.com	*99***1#	bt	bt	
BT Mobile Customer Value	btmobile2.bt.com	*99***1#	bt	bt	
Jersey Telecom	pepper		abc	abc	
Jersey Telecom	pepper	*99#			
Manx Telecom	internet				
Meteor	isp.mymeteor.ie		my	meteor	
O2 (1) with contract	mobile.o2.co.uk		web	password	
O2 (2) with contract	mobile.o2.co.uk	*99# OR *99***1#	o2web OR faster	password	DNS Address (if needed): 193.113.200.201
O2 (1) faster, with contract	mobile.o2.co.uk		faster	password	

O2 (2) faster, with contract	mobile.o2.co.uk	*99# OR *99***1#	faster OR o2web	password	DNS Address (if needed): 193.113.200.201
O2 pre-pay	payandgo.o2.co.uk		payandgo	payandgo	
Orange Pay Monthly	orangeinternet		user	pass	
Orange Pay and Go	orangewap		Multimedia	Orange	
T-Mobile	general.t-mobile.co.uk		user	pass	
Tesco Mobile	prepay.tesco-mobile.com		tescowap	password	
Virgin Mobile (1)	goto.virginmobile.com		user	[space]	
Virgin Mobile (2)	goto.virginmobile.com	*99#	Leave blank	Leave blank	Authentication: PAP
Vodafone	ppbundle.internet		web	web	
Vodafone contract	internet		web	webs	
Vodafone contract	wap.vodafone.co.uk		wap	wap	
Vodafone pre-pay	pp.vodafone.co.uk		wap	wap	
Three UK	three.co.uk		guest	guest	
Three Ireland	3ireland.ie		guest	guest	

Appendix B: Troubleshooting Tips

The following are some problems you may experience and some possible solutions to remedy the situation.

Problem

After connecting the Modem/Router to a computer, the connected Ethernet (LAN) port light does not blink.

Solution

- Check that the Modem/Router's power cube is plugged into a working power outlet and into the Modem/Router. The Modem/Router's Status light should be on and blinking.
- Make sure the PC is ON
- Make sure the Ethernet cable is correctly plugged into the PC and into the Modem/Router's Ethernet port. Try replacing the Ethernet cable with another cable.
- Check that the PC's Ethernet (LAN) port is enabled and working properly. (Refer to your PC's documentation for details.)

Problem

I followed the instructions for connecting the Modem/Router and entered **http://192.168.2.1** in my web browser's address bar, but I cannot access the Modem/Router. (The **Status** page does not appear).

Solution

- Verify that power is on to the Modem/Router and that the Ethernet cable is plugged between your Modem/Router and your computer's Ethernet (LAN) port.
- Manually reset the Modem/Router. Insert a paper clip into the RESET opening on the front panel, then press and hold down for 10 seconds. Then power off your computer and power it back on. After you've done that, re-enter **http://192.168.2.1** in your web browser's address bar.
- The computer connected to the Modem/Router must have its TCP/IP parameters setup to use DHCP (also called Dynamic IP). Check that your computer is setup to use DHCP.

Problem

I am unable to connect to the Internet OR I used the Setup Wizard to set up the Router and saw the message “Connection to Internet failed”.

Solution

There are several issues that could cause this problem. Check these items:

- If you used the Setup Wizard and the connection to the Internet failed, try opening a browser and going to a website. If this works, then your setup is OK.
- Verify that the Status light on the Modem/Router is on and blinking. If it is off, check that the Modem/Router is plugged into a working power outlet. If the light does not turn on, make sure there is power going to the outlet you are using. If the unit still doesn't work, contact Zoom Technical Support. See [Appendix D](#) for contact information.
- If you are using a wireless device, try connecting a computer directly to one of the Modem/Router's Ethernet (LAN) ports. If a computer directly connected to the Modem/Router works, then the problem is with your wireless connections. See the [wireless troubleshooting tip](#).
- If you cannot access the Internet with a computer directly connected to one of the Modem/Router's Ethernet (LAN) ports, check your Ethernet connection. Most computers have a power light next to the Ethernet jack to indicate the Ethernet cable is properly connected. Verify that this light is on and that one of the Ethernet light on the front of the Modem/Router is on. If the Ethernet light is off on either the Modem/Router or on the computer, verify that the cable is properly pushed in. If the light still doesn't turn on, you should try another Ethernet cable.
- Try turning your computer off and then on. This ensures that your computer gets a correct IP address from the Modem/Router.

If you are using Mobile Broadband to connect to the internet please see [Troubleshooting your Built-in 3G+ Modem Connection](#).

Problem

My wireless computer/devices are not connecting to the Internet.

Solution

Try the following:

- Verify that a “wired” computer can access the Internet.

If it cannot, try the steps outlined in the previous troubleshooting tip.

If the wired computer can access the Internet, reboot the device(s) on your wireless network (this will allow for the computers to release and renew their IP addresses) and try to access the Internet again.

If you still cannot connect to the Internet wirelessly, continue below.

You should also verify that the correct wireless network name is selected as the wireless network. By default the wireless network name is Zoom_xxxxxx where xxxxxx is 6 random alphanumeric characters. If it is not, then you are connected to the wrong network. To verify the network, follow the instructions in [Chapter 4, Connecting Devices Wirelessly to the Modem/Router](#).

- Check your wireless security settings on your Router and verify that your device is using the same settings.
- Check the signal strength of your wireless connection. Most wireless adapters have some type of signal strength meter that shows how strong your wireless signal is. **Windows users**, click the **Wireless** icon in your system tray to check signal strength. If your signal strength is not strong enough, try the following:
 - Move the Modem/Router to another area.
 - Move the device trying to access the Modem/Router to a different location, ideally closer to the Modem/Router.
- Change the wireless channel. In the unlikely event that you experience performance issues with your wireless network, you may want to set your network up on a channel that's different from the factory-set channel of 10. To do that, follow these steps:
 - 6 In the Web browser address bar, type the Modem/Router 's default IP address, **http://192.168.2.1** and then click **Enter**.
 - 7 In the **System Password** field, type **admin** and then click **Login**.
 - 8 When the **ADMINISTRATOR'S Main Menu** opens, click **Advanced** on the Toolbar.
 - 9 On the **Basic Settings** page, click **Wireless** on the left-side menu to open the **Wireless** page.
 - 10 On the Wireless page, from the **Channel** drop-down menu, select a channel number for your network that is not being used by another network. If possible, try to maintain a 5-channel difference between your network and other nearby networks. You may want to try, for example, channel 1 or 6.
 - 11 Be sure to click **Save** after you change the channel. All devices connecting wirelessly to the Modem/Router will automatically switch to the new channel.
- If you are using a computer with a wireless network card installed, access the network card's software and verify that it is connected to the **Zoom_xxxxxx** network (or whatever you changed the SSID/network name to) and that the signal strength is adequate. Refer to the documentation that came with the network card if you need help doing this.
- Refer to the documentation provided with your network device or contact its manufacturer for assistance.

Problem

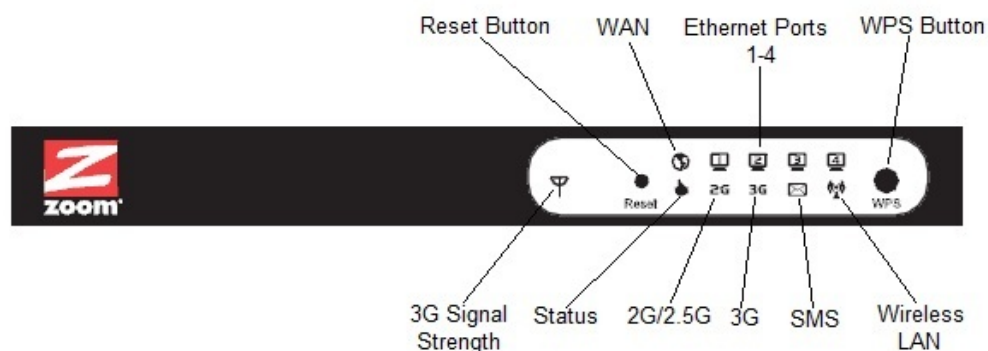
When I click on a page I receive a “Modem isn’t Ready! Please check that the SIM card is inserted” error.

Solution

There are several issues that could cause this problem. Check these items:

- Your SIM card is not inserted into the Modem/Router. Please insert your SIM card.
- You inserted your SIM card while the modem was powered on. The SIM card should be inserted when the Modem/Router is powered off. Turn off the power to the unit, then turn it back on to ensure the SIM card is read correctly.

Appendix C: Front Panel Lights



	Status	Description
3G Signal Strength	Flashing Red	Modem/Router is not connected
	Flashing Amber	Connecting
	Red	Connected Signal strength is poor
	Flashing Red Quickly	Roaming onto another network Signal strength is poor
	Amber	Connected Signal strength is OK
	Flashing Amber Quickly	Roaming onto another network Signal strength is OK
	Green	Connected Signal strength is good
	Flashing Green Quickly	Roaming onto another network Signal strength is good
Status	Flashing Green	Device working normally
2G/2.5G	Green	2/2.5G connection established
	Flashing Green	Data being sent over 2/2.5G Network

3G	Green	3G+ connection is established
	Flashing Green	Data being sent over 3G+
SMS	Green	SMS storage is full
	Flashing Green	You have an unread SMS message
WAN	Green	WAN port is active
	Flashing Green	Data being sent out the WAN port
Ethernet Ports	Green	Ethernet port is connected
	Flashing Green	Data being sent over the Ethernet connection
Wireless LAN	Green	Wireless LAN is on
	Flashing Green	Data being sent over wireless LAN
	Quickly Flashing Green	Device is in WPS mode

Appendix D: Registering Your Product and Getting Help

Zoom supports this Modem/Router. If you need assistance, please contact Zoom directly. We encourage you to register your product and to notice the many support options available from Zoom. Please go to **www.zoomtel.com** and select **Technical Support**. From there you can register your new Modem/Router, contact our technical support experts, use our SmartFacts™ intelligent database, and get warranty information.

If you need to contact Zoom Customer Support, you can call us by dialing our main support center in the USA or our support center in the UK.

USA: (617) 753-0965

U.K.: London: +44 2033180660

Manchester: +44 1618840074

Limited Warranty

Zoom Telephonics, Inc. (hereinafter “Zoom”) warrants this product against defects in material and workmanship for a warranty period of one year. The one year warranty may be extended only by Zoom as required by local law in the country where this modem is sold by Zoom. This warranty applies to the original end-user purchaser.

For all Zoom products other than software, Zoom will, solely at its option, repair or replace this product with a functionally equivalent new or factory-reconditioned product during the warranty period. The consumer will deliver the product to Zoom. All transportation risks and costs in connection with this warranty service are the responsibility of the consumer.

Zoom will replace software at no charge if there is a defect in materials or workmanship for a period of 30 days from date of original retail purchase, provided the defective software is returned to Zoom. Shipments from Zoom will normally be via U.S. Mail. Software products supplied by Zoom are sold “as is,” without warranty, either expressed or implied, as to function, application, merchantability, performance, and quality.

Zoom is not responsible for incidental or consequential damages, and is not responsible for damages resulting from the breach of any expressed or implied warranty. Zoom is not responsible for any costs of recovering, reprogramming, or reproducing any programs or data stored or used with the Zoom products, damage to property, and to the extent permitted by law, damages for personal injury.

This warranty is in lieu of all other warranties, expressed or implied. We do not assume or authorize assumption for us of any other warranty expressed or implied. Some states and countries do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusions may not apply to you.

This warranty does not apply if the Zoom product has been damaged by accident, abuse, lightning or other natural disasters, misuse or misapplication, or if it has been modified without the written permission of Zoom, or if any serial number has been removed or defaced.

This warranty shall not be applicable to the extent that any provisions of this warranty are prohibited by any federal, state, or municipal law that cannot be preempted. This warranty gives you specific legal rights, and you may also have other rights that vary from state to state

or country to country.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 5022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC.

Declaration of Conformity

	Declaration of Conformity Déclaration de conformité Konformitätserklärung Dichiarazione di conformità Declaração de Conformidade Konformitetsdeklaration	Overensstemmelseserklæring Conformiteitsverklaring van de EU Δήλωση Συμμόρφωσης Deklaracja zgodności Declaración de conformidad Cam kết về sự tuân thủ ở Châu Âu
Manufacturer/Producent/Fabrikant/ Constructeur/Hersteller/Κατασκευαστής / Fabbricante/ Fabricante/Tillverkare/ Nhà sản xuất	Zoom Telephonics, Inc. 207 South Street Boston, MA 02111 USA / 617-423-1072 www.zoomtel.com	
Brand/Varemærke/Merk/Marque/Marke / Μάρκα/Marchio/Marke/Marca/Thương hiệu	Zoom Wireless-N Router w 3G+Modem &Voice	
Type/Typ/Mάρκα/Tipo/Kiểu mẫu	Model 4530 Series 1098	

The manufacturer declares under sole responsibility that this equipment is compliant to Directive EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC via the following. This product is CE marked.

Producenten erklærer under eneansvar, at dette udstyr er i overensstemmelse med direktivet EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC via følgende. Dette produkt er CE-mærket.

De fabrikant verklaart geheel onder eigen verantwoordelijkheid dat deze apparatuur voldoet aan Richtlijn EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC op grond van het onderstaande.

Dit product is voorzien van de CE-markering. Le constructeur déclare sous son entière responsabilité que ce matériel est conforme à la Directive EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC via les documents ci-dessous. Ce produit a reçu le marquage CE.

Hiermit erklärt Zoom die Übereinstimmung des Gerätes modem mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC. Dieses Produkt ist das gekennzeichnete CE.

Ο κατασκευαστής δηλώνει με αποκλειστική του ευθύνη ότι αυτό το προϊόν συμμορφώνεται με την Οδηγία EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC μέσω των παρακάτω. Αυτό το προϊόν φέρει τη Σήμανση CE.

Il fornitore dichiara sotto la sola responsabilità che questa apparecchiatura è compliant a EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC direttivo via quanto segue. Questo prodotto è CE contrassegnato.

Producent stwierdza że to urządzenie zostało wyprodukowane zgodnie z Dyrektywą EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC. Jest to potwierdzone poprzez umieszczenie znaku CE na urządzeniu.

O fabricante declara sob sua exclusiva responsabilidade que este equipamento está em conformidade com a Directiva 1 EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC através do seguinte. Este produto possui Marcação CE.

El fabricante declara bajo su exclusiva responsabilidad que este equipo satisface la Directiva EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC por medio de lo siguiente. Este producto tiene marca CE.

Nhà sản xuất cam kết với trách nhiệm của mình là thiết bị này tuân theo Hướng dẫn EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC thông qua các mục sau. Sản phẩm này được đánh dấu là CE.

EN 60950-1:2006/A11:2009 / IEC 60950-1:2005+A1:2009
EN 301 908-1 V4.2.1:2010-03 / EN 300 328 V1.7.1 :2006
EN 301 511 (TS151 010-1 V6.6.0 (2006-1) 3GPP TS 51.010-1 Version 6.6.0 Release 6)
EN50385:2002 / EN 62311 :2008



Director, /Direktør, /Director, /Directeur /Direktør, /Διευθυντής,
/Direttore, /Dyrektor /Director, /Director, Đốc

Paul Prohodski
22 August, 2012
1098/TF, Boston, MA, USA

U.S. FCC Part 15 Emissions Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Operations in the 2.4GHz band are restricted to indoor usage only.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.